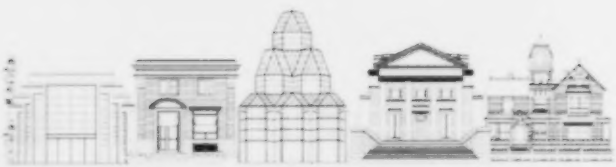
LA VITRINE VIRTUELLE :

Exposer en toute sécurité la richesse visuelle des musées

Troisième édition

Rapport rédigé pour le



Réseau canadien d'information sur le patrimoine

par

Peter H. Roosen-Runge, Ph. D.,
Université York

et

Anna P. Roosen-Runge,
Analecta Research & Resources,

Février 2002

Traduit de l'anglais par Benoît Thouin, *trad. a. (Canada)*

©Sa majesté la Reine du chef du Canada, 2003
Imprimé au Canada

Données de catalogage avant publication de la Bibliothèque nationale du Canada

Roosen-Runge, Peter H.

La vitrine virtuelle : exposer en toute sécurité la richesse visuelle des musées

3e éd.
Publ. aussi en anglais sous le titre : The Virtual Display Case.
Comprend des références bibliographiques.
ISBN 0-660-96664-6
No de cat. Co61-17/2003F

1. Numérisation.
2. Objets d'art – Conservation et restauration.
3. Biens culturels – Protection.
4. Museés – Méthodes de conservation.
I. Roosen-Runge, Anna P.
II. Réseau canadien d'information sur le patrimoine.
III. Titre.
IV. Titre : Exposer en toute sécurité la richesse visuelle des musées.

AM145.R66 2003 069'.53 C2002-980065-X

Réseau canadien d'information sur le patrimoine (RCIP)
15, rue Eddy (15-4-A)
Gatineau (Québec) K1A 0M5

Téléphone : (819) 994-1200
1 800 520-2446
Télécopieur : (819) 994-9555
Courriel : service@rcip.gc.ca
URL : www.rcip.gc.ca

Un mot du Réseau canadien d'information sur le patrimoine (RCIP)

Cette troisième édition de *La Vitrine virtuelle* aborde des techniques originales et nouvelles, souvent désignées par le vocable « gestion numérique des droits d'auteur », qui servent à protéger des images numériques dans un environnement en ligne. Cet ouvrage ne prétend pas couvrir le sujet de manière exhaustive. Premièrement, le RCIP et les auteurs de ce rapport ont concentré leur attention sur les images en tant que forme de propriété intellectuelle qui peut bénéficier de systèmes de gestion numérique des droits d'auteur. Les établissements du patrimoine traitent cependant bien d'autres formes de propriété intellectuelle dans un environnement en ligne. La production d'expositions en ligne fait aussi intervenir des fichiers audio et audio-visuels, des images en trois dimensions et d'autres médias souvent plus complexes que des images en deux dimensions d'objets d'une collection. Deuxièmement, les techniques peuvent avoir évolué entre la préparation et la publication de ce rapport. Nous avons cru néanmoins nécessaire de publier celui-ci, ne serait-ce que pour offrir un point de départ aux professionnels des musées qui se lancent dans la gestion numérique des droits d'auteur sur les images de leur établissement.

Les spécialistes débattent depuis longtemps sur la capacité d'Internet à atteindre ses objectifs, en particulier dans le secteur de la musique. On dit dans le domaine que tout moyen technique qui peut être mis au point peut aussi être piraté ou détourné. Les réalisateurs de contenu sur différents supports doivent combattre de nouvelles formes de piratage, mais ils recherchent eux-mêmes de nouveaux moyens techniques susceptibles de les assister dans leur lutte. Les réalisateurs de produits essaient de répondre aux besoins du marché, et l'on entend donc beaucoup parler de leurs nouveaux produits. Mais on met l'accent sur la « prochaine grande réalisation » plutôt que sur l'analyse et l'évaluation systématiques de la technologie et sur l'élaboration des normes nécessaires pour obtenir des solutions à long terme. C'est dans ce contexte que le RCIP fait paraître cette troisième édition de *La Vitrine virtuelle*, afin de procurer au milieu du patrimoine un guide solide à propos de la forme la plus fondamentale de contenu numérique sur le patrimoine, à savoir l'image.

Rina Elster Pantalony
Conseillère juridique, RCIP

Table des matières

8 **Avant-propos de la troisième édition**

9 **Remerciements**

10 **1 Aperçu et sommaire**

12 **2 Le contexte**

14 2.1 Musées en ligne
16 2.2 Conservation et images numérisées
16 2.3 Obligations et risques
18 2.4 L'exploitation sous licence : un moyen de sensibilisation
22 2.5 La normalisation des contrats de licence

24 **3 Systèmes de gestion numérique des droits d'auteur**

24 3.1 Conteneurs et superdiffusion
25 3.2 Systèmes de gestion des droits d'auteur
26 3.2.1 *ContentGuard*
27 3.2.2 *InterTrust*
28 3.2.3 *RightsMarket*
28 3.2.4 *OnDisC*
29 3.3 La technologie de diffusion comme moyen de protéger les droits de propriété intellectuelle
30 3.3.1 *Alchemedia* et *Vyoufirst*

32 **4 Les techniques de protection**

32 4.1 Types de filigrane
33 4.1.1 Filigranes visibles
34 4.1.2 Filigranes invisibles
36 4.1.3 Filigranes fondés sur la méthode DCT
37 4.1.4 Suivi de l'utilisation
37 4.2 Le chiffrage
39 4.2.1 Les signatures d'authentification
40 4.2.2 Logiciel ou matériel
40 4.2.3 Contournement du chiffrage par des moyens logiciels
41 4.2.4 Lien entre compression et chiffrage
42 4.3 Techniques d'incorporation de données
42 4.3.1 Cognicity
42 4.3.2 Digimarc
44 4.3.3 MediaSec
45 4.4 Techniques de conteneurs étanches
45 4.4.1 Conteneurs *DigiBox* d'InterTrust
46 4.4.2 *RightsPublish* de RightsMarket

48 **5 À l'horizon**

48 5.1 Métadonnées sur les droits d'auteur et XML
50 5.2 JPEG2000
51 5.3 MPEG-4

54 **Sources**

61 **Fournisseurs et organismes**

Avant-propos de la troisième édition

Le rythme rapide et soutenu de l'innovation technologique réduit considérablement la vie utile de la plupart des sommaires ou études sur les moyens techniques liés aux images numérisées et à leur protection. Il suffit de quelques mois pour que des références bibliographiques deviennent périmées, que des entreprises offrant des produits dans ce domaine disparaissent ou changent de nom, et que surviennent de nouveaux développements d'un intérêt certain.

Cette édition constitue une révision substantielle de la version précédente. Nous avons supprimé les références à des questions qui semblent maintenant moins importantes ou à des moyens techniques qui ont été remplacés, et nous avons fait place à de nouveaux développements dans l'industrie de l'information et dans la gestion numérique des droits.

Le Web est un outil incroyablement puissant, capable d'apporter au lecteur une information à jour sur la gamme complète des questions d'ordre technique et politique abordées dans ce rapport. C'est pourquoi nous avons donné lorsque c'était possible des adresses URL à titre de référence. Par contre, l'accès immédiat et l'absence de structure rigide qui rendent le Web si utile en font aussi une source d'information très éphémère qui peut entraîner beaucoup de frustration. Nous avons essayé de vérifier que tous les liens cités dans ce document sont valables, mais cela ne durera pas longtemps. Cependant, même si certains liens ne sont plus valables, les sites eux-mêmes peuvent toujours contenir de l'information utile. D'autre part, avec une utilisation judicieuse d'outils de recherche, le lecteur pourra trouver d'autres sources d'information plus à jour.

Remerciements

Nous remercions sincèrement Rina Elster Pantalony pour son intérêt et son aide à la rédaction de cette monographie, ainsi que le Professeur Theodore Wilcox pour sa contribution à la section 5.2.

Avis de marque de commerce

XrML, eXtensible Rights Markup Language et le logo XrML logo sont des marques de commerce de ContentGuard Holdings, Inc. Copyright © 2000, ContentGuard Holding, Inc. Tous droits réservés.

RightsXML[MC] est une marque de commerce de TrustData Solutions Corp.

1 Aperçu et sommaire

La présente étude porte sur les questions d'ordre technologique liées à la préservation et à la diffusion d'*images numérisées* de collections de musées. Elle explore plus particulièrement le lien qui existe entre les technologies d'affichage et de réseau d'une part et les questions de propriété intellectuelle d'autre part. L'étude s'appuie sur une recension des documents utiles et des produits actuellement disponibles dans le commerce, ainsi que sur les travaux sur la diffusion multimédia et la gestion des droits menés par le consortium *OnDisC Alliance* au collège Sheridan, à Oakville, en Ontario.

Comme l'indique le titre de cet ouvrage, nous nous intéressons principalement aux conséquences de la diffusion d'images numériques, obtenues généralement en numérisant des photographies, en prenant des photos à l'aide d'un appareil photographique numérique ou encore par Internet. Mais avec l'évolution de la technologie d'Internet, il devient de plus en plus commode de diffuser des fichiers beaucoup plus volumineux contenant des extraits sonores et des séquences vidéo. C'est pourquoi nous avons étendu la portée de notre étude afin d'inclure certains aspects techniques et questions de propriété intellectuelle concernant le multimédia en général. Dans le passé, à cause de la taille des fichiers multimédias et de la bande passante qu'ils exigeaient, la publication ne pouvait se faire à un coût raisonnable que sur disque optique compact. Aujourd'hui, on peut supposer que presque *toute* diffusion de matériel multimédia au grand public se fait par Internet.

Nous constatons que si les techniques numériques permettent de mettre au point des méthodes nouvelles et puissantes de conservation de textes et d'images et de diffusion de reproductions, elles engendrent en même temps d'épineux problèmes de propriété intellectuelle. En effet, il y a incompatibilité entre les valeurs que représentent les musées en tant qu'institutions culturelles et le marché, tout comme il y a un conflit entre les valeurs altruistes qui ont permis à Internet de croître et le désir de protéger les droits économiques inhérents, de par la loi, aux œuvres créées.

Il semble évident que le seul fait de modifier la loi sur le droit d'auteur et d'en étendre la portée ne résoudra pas ces problèmes, pour autant que ceux-ci puissent être résolus. En fait, à certains égards, à cause des incertitudes venant de la loi et des frais liés à toute poursuite judiciaire, que ce soit à titre de plaignant ou de défendeur, les modifications à la loi sur le droit d'auteur ont rendu la situation plus complexe tant pour les musées que pour les titulaires de droits d'auteur, de sorte que des projets sont abandonnés ou ne sont plus considérés réalisables pour les musées en raison de la complexité et du coût de l'affranchissement des droits. Par conséquent, les musées sont privés de redevances et de revenus, et les œuvres et objets qu'ils possèdent sont moins utilisés à des fins éducatives et créatrices. Certaines difficultés peuvent être aplanies par diverses formules d'utilisation sous licence, comme cela est répandu dans le domaine du logiciel. Cependant, les conditions d'utilisation sous licence doivent être acceptables pour les usagers, et les émetteurs de licence doivent veiller à éduquer les usagers aux notions de base de la propriété intellectuelle.

Certains considèrent que l'exploitation sous licence, même dans les cas où il y a enregistrement, protège mal les biens esthétiques qui conservent leur valeur dans le temps. C'est pourquoi les moyens proposés pour prévenir ou décourager la copie d'images numérisées attirent beaucoup l'attention, et que des techniques comme le filigrane, le chiffrage, les signatures numériques et les empreintes d'identification ont été mises au point et sont maintenant commercialisées. Des

techniques récentes telles que la description normalisée d'objets par des métadonnées, l'intégration du chiffrage dans des algorithmes de compression d'images et la présence d'identificateurs permanents d'objets dans leur présentation sous différentes formes illustrent une tendance en vertu de laquelle les logiciels employés pour créer et transmettre un contenu numérique doivent tenir compte des droits et les protéger dans la structure même des objets sous forme numérique.

Dans leurs formes actuelles, les filigranes, les signatures et les empreintes d'identification ont surtout une valeur dissuasive. Le chiffrage permet une sécurité élevée, mais même dans ce cas, la protection n'est jamais absolue, et les musées qui adoptent ces techniques doivent composer avec le fait qu'il y aura toujours atteinte au droit d'auteur, encore qu'à une échelle réduite et sans conséquences financières sérieuses. Tout compte fait, la stratégie la plus appropriée à court terme consiste à alléger le plus possible le fardeau que représentent les techniques de protection, tout en respectant les dispositions de la loi, et à se protéger contre les pertes économiques grâce à des contrats de licence simples, conçus et appliqués en direct pour des œuvres déterminées et des périodes précises.

À terme, ce qui comptera pour les usagers sera la facilité d'accès, la variété et l'exhaustivité dans un domaine donné. Comme c'est un environnement réseau largement décentralisé qui réalise le mieux ces conditions — l'usager n'a pas à acheter d'objets physiques tels que des disquettes ou des disques optiques compacts dont le contenu est figé, mais seulement des documents et des représentations exploitables sous licence —, il est alors absolument nécessaire que les systèmes informatiques soient capables de gérer les droits sur les représentations numériques. Une technique logicielle sur laquelle de tels systèmes peuvent être fondés est en phase active de développement et de mise en exploitation, sous la forme d'*architectures logicielles modulaires*. Le *Component Object Model* (COM) de Microsoft, *CORBA*, du *Object Management Group* et *JavaBeans* de Sun Microsystems sont des exemples de tels systèmes. À partir des composantes définies dans ces architectures logicielles, les *systèmes de gestion numérique des droits d'auteur* (ou SGDN pour systèmes de gestion des droits numériques) créent des *conteneurs sûrs* dont le contenu est chiffré et recèle l'information et les mécanismes de mise à jour employés pour appliquer les modalités du contrat d'exploitation sous licence, consigner les données sur l'utilisation, transmettre les données sur les redevances aux sociétés de gestion du droit d'auteur et émettre des factures aux consommateurs. Le *Windows Media Rights Manager* de Microsoft [Microsoft, 2000], dans lequel « des objets du modèle COM servent à protéger les fichiers et à émettre des licences » est un exemple de SGDN.

À court terme, il semble que la technique des conteneurs sera surtout appliquée aux livres numériques et à la diffusion numérique de musique populaire. Nous croyons toutefois qu'elle revêt une grande importance pour les musées puisqu'elle résoudra vraisemblablement le problème de la rediffusion en faisant de la copie et de la retransmission de l'information, que les techniques de protection actuelles tentent d'empêcher, **non plus un acte illicite, mais bien un acte souhaitable**, grâce à la « superdiffusion ». Si les avantages escomptés de la superdiffusion se concrétisent effectivement, on pourra peut-être réaliser l'équilibre entre l'importance d'offrir une information esthétique et éducative de manière coopérative et altruiste d'une part, et le besoin de rémunérer les créateurs d'autre part. Il sera alors possible de présenter, ne serait-ce que virtuellement, les trésors de chaque musée à un public considérablement élargi.

2 Le contexte

Les musées ont de bonnes raisons de croire qu'ils sont au seuil d'un « âge d'or ». Au cours des dernières décennies, ils ont effectivement réussi à concevoir des expositions et des installations alliant photographies, textes, films, vidéos et extraits sonores pour éduquer et divertir. Et maintenant, c'est avec une rapidité hallucinante que ces mêmes techniques trouvent une expression nouvelle et beaucoup plus puissante dans le domaine numérique, qui permet de mettre l'exposition ou l'installation à la portée du « visiteur virtuel » à l'école, dans une bibliothèque publique ou à la maison dans un pays lointain.

En même temps, l'expression des droits de propriété pour la publication, l'exposition ou la représentation d'œuvres créées, y compris toutes les formes de traitement d'images, est de plus en plus vigoureuse et complexe, si bien qu'on est en droit de se demander ce que les musées peuvent faire pour saisir ces nouvelles possibilités « en or ». La différence entre ce qui est techniquement possible et ce qui est pratique, est une réalité que les professionnels des musées connaissent bien. Cette frustration a été exprimée pendant une réunion dans le cadre du *Digital Image Access Project* (Projet d'accès aux images numérisées) [1995] : « De tous les besoins du domaine des arts et des sciences humaines, le plus grand vise l'accès en direct à des images. Nous savons qu'il existe des milliards d'images et que celles-ci sont à toutes fins pratiques inaccessibles. Nous avons en grande partie les moyens techniques de les saisir et de les afficher... » [traduit de l'anglais]. Cependant, même si des fonds étaient dégagés pour la numérisation et l'indexation, la question des droits intellectuels viendrait assombrir la perspective d'un accès universel à de vastes archives d'images.

> « Rien n'a nui au développement créatif de programmes multimédias interactifs et éducatifs autant que les questions de propriété intellectuelle. La seule perspective d'une suite interminable de lettres pour demander la permission d'utiliser une image donnée a empêché la réalisation de nombreux projets. » [traduit de Trant, 1994]

La solution pratique à ce problème créé par la technologie viendra en partie de la technologie elle-même. Les musées employaient des vitrines d'exposition classiques pour mettre leurs collections à l'abri des dommages et du vol tout en permettant aux visiteurs d'en voir le plus possible le contenu. À mesure que les musées feront de plus en plus appel aux techniques numériques pour créer des archives d'images et des expositions multimédias, ils pourront exploiter de nouvelles formes de « vitrines », c'est-à-dire des logiciels qui permettront aux musées d'exposer un maximum de contenu dans des réseaux facilement accessibles, tout en protégeant les images et les expositions contre la copie et la publication non autorisées.

Heureusement, les outils et les techniques dans ce domaine évoluent rapidement afin de répondre aux besoins commerciaux des marchés en expansion pour toutes les formes de médias numériques, plus particulièrement par la présence de nouveaux médias dans les réseaux, et certaines de ces nouvelles méthodes sont pertinentes pour la protection d'objets muséologiques en ligne. Cela confirme une tendance, relevée par Gurrian [1995], qui fait remarquer que les musées seront désormais considérés comme d'autres entités dans les classifications nouvelles, qui comprennent non seulement les bibliothèques, services d'archives et écoles traditionnels, mais aussi les « entrepôts technologiques », par exemple les banques d'images.

Des initiatives actuelles d'envergure nationale encouragent le lancement et la poursuite de projets de numérisation, qui stimulent à leur tour la mise sur pied de bibliothèques de dépôt numériques. À mesure que ces bibliothèques de dépôt numériques croissent, leur contenu devient de plus en plus utile, ce qui incite davantage les participants à y verser des documents multimédias tels que des extraits sonores et des images autrefois inacessibles au grand public. Un exemple canadien d'une telle initiative est le projet BELLE, qui vise la définition et la mise sur pied d'une base de données consultable de contenu multimédia, à l'intention d'institutions d'enseignement postsecondaire, pour l'enseignement à distance. Les participants à ce projet sont des universités et des collèges de partout au Canada, reliés par une infrastructure de serveurs multimédias qui met l'accent sur la rapidité et la qualité du service. Le projet BELLE offre aux usagers, par le truchement d'un système à large bande, l'accès à des séquences vidéo à grande résolution ainsi qu'à des fichiers d'images en trois dimensions dont la taille empêche le visionnement à l'aide des réseaux conventionnels. En mettant l'accent sur l'accessibilité, la facilité de consultation, la souplesse d'utilisation et la stabilité des ressources de réseau, le projet BELLE contribuera à stimuler la mise sur pied par la communauté muséale canadienne de programmes accessibles d'éducation et de diffusion par Internet.

Un autre exemple est celui des projets Info2000 de la Commission européenne, qui visent à stimuler le développement et l'utilisation de contenu multimédia. Un de ces projets est celui des Archives visuelles européennes (ou EVA pour *European Visual Archive*) [van Horik, 2001], où une approche détaillée et systématique permet d'accroître l'accès aux collections de photographies historiques au moyen de la documentation et de la numérisation. Dans ce cas, l'exploitation commerciale n'est pas une préoccupation importante — l'objectif est plutôt de créer un système « au seuil de participation peu élevé » permettant aux collections européennes d'images « d'être mises en contact avec un énorme réservoir de consommateurs potentiels » [traduit de l'anglais].

Les musées devront s'adapter à la présence dans Internet de fournisseurs commerciaux auxquels il est facile d'avoir accès et qui cherchent à vendre des images de grande qualité à prix raisonnable non seulement aux graphistes et aux éditeurs, mais aussi aux écoles et, à terme, aux particuliers. Storm [1995] presse les bibliothèques et les services d'archives de « prendre du recul... et d'analyser la façon dont ils seront et sont maintenant touchés par l'avènement de services commerciaux d'information en réseau » [traduit de l'anglais].

Un exemple intéressant de service de ce genre est celui de Corbis [Lieber, 1995] qui, fort de la richesse de Bill Gates, met tout en œuvre pour acquérir des droits « électroniques », parfois exclusifs, pour les images numérisées des fonds de musées d'art et d'archives photographiques comme les photographies d'Ansel Adams. Avec l'achat de la totalité des archives Bettmann en 1995 et l'achat en 1999 de l'agence de photographes de presse Sygma, Corbis détient maintenant les droits sur plus de 65 millions d'images, dont 2,1 millions sous forme numérique [Reuters, 1999]. Comme le fait remarquer M. Hallacy, « Bill Gates a dans les faits acquis les droits sur le registre photographique de l'histoire... Ces droits comprennent la capacité de notre culture de faires des reproductions de nous-mêmes. » [traduit de l'anglais] Corbis détient les droits sur les archives numériques de plusieurs grands musées, dont le musée de l'Hermitage à Saint-Pétersbourg, la *National Gallery* à Londres, le *Seattle Museum of Art*, la *National Gallery of Art* et la *Corcoran Gallery* à Washington, D.C. [Hallacy, 2000]. D'autres projets de Corbis comprennent *Corbis Sharpshooters*, spécialisé dans les photographies qui portent sur des personnes, des modes

de vie et la nature, et *Corbis Saba*, qui représente des photographes rédactionnels et des portraitistes. En janvier 2002, Corbis a acheté l'entreprise d'images animées Sekani (www.corbis.com).

À titre de comparaison, la collection numérique du consortium AMICO (*Art Museum Image Consortium*) compte environ 65 000 images d'art mises à la disposition de ses membres qui participent à un accord de coopération en matière de numérisation, de licence et de diffusion. Le Musée virtuel du Canada met gratuitement à la disposition du grand public environ 200 000 images des collections de ses musées membres. Les accords qui lient les membres décrivent les rôles et les responsabilités dans le cadre de ce projet de coopération.

2.1 Musées en ligne

Des musées de toutes tailles montent avec grand enthousiasme des pages Web, et ce phénomène s'étend rapidement. Pour un petit musée comme le *Berea College Museum*, le motif est clair : « rejoindre le grand public et les étudiants ». Comme Chris Miller l'indique dans *MUSEUM-L* (9 avril 1996) :

> « L'exposition en ligne est un moyen viable d'augmenter son auditoire dans de nouveaux secteurs. Nous sommes un petit musée de collège en région rurale et nous nous concentrons sur l'histoire et la culture des Appalaches. Presque tous les internautes qui visitent la « *Gallery V* » (V pour virtuel) de notre musée en ligne ne se seraient pas présentés en personne. Presque 25 % de nos visiteurs en ligne sont étrangers. Il y a des gens en Équateur qui s'intéressent à la culture des Appalaches et qui ne peuvent pas venir à notre musée. Pour eux, mieux vaut une visite virtuelle que pas de visite du tout. » [traduit de l'anglais]

Pour leur part, les musées plus importants peuvent sans doute remettre en question la valeur des expositions virtuelles par rapport à celle d'une visite réelle mais, malgré tout, ils sont toujours de plus en plus nombreux à faire leur apparition en ligne. « Le Web offre au Musée [canadien des civilisations] un moyen relativement peu coûteux de diffuser ses ressources d'information à de nombreux publics. [...] son utilisation se répand dans le système d'éducation grâce à des projets comme Rescol. » [traduit de Alsford, 1994]

À Taïwan, le Musée national du palais a créé un site Internet qui propose des visites virtuelles pour mettre en lumière ses collections et ses expositions. À partir d'un plan cliquable, le visiteur est amené dans des salles ou des zones où il peut se promener et regarder à 360 degrés, à l'aide du plugiciel *QuickTime* de son navigateur. Il peut même sortir du taxi dans lequel il est arrivé de manière virtuelle! Une peinture virtuelle du palais lui-même est accompagnée d'une description détaillée de la peinture, de son état actuel et d'une explication de son contexte comparable au contenu de l'audioguide d'une exposition réelle.

La décision de l'ICANN (*Internet Corporation for Assigned Names and Numbers*) de mettre sur pied le domaine de premier niveau *.museum* témoigne de la place de la communauté muséale dans Internet et le Web.

Il y a à l'heure actuelle un intérêt pour le financement de programmes de création de contenu culturel en ligne. La proposition d'initiative *Culture Online* du ministère de la Culture, des Médias et

des Sports au Royaume-Uni vise à « utiliser la technologie numérique pour élargir l'accès aux ressources des arts et du secteur culturel... » [Traduit de www.cultureonline.gov.uk].

Au Canada, le *Musée virtuel du Canada* (MVC) comporte une collection désignée de contenu de grande qualité mis sur pied par des musées et leurs partenaires. Le MVC est une initiative du programme de financement *Culture canadienne en ligne*, créé afin de « rehausser les capacités des industries, des organismes, des créateurs et des communautés culturels du Canada à produire du contenu culturel numérisé et à l'offrir sur l'Internet (*sic*), et ainsi promouvoir la richesse de la culture, de l'histoire, des arts, du patrimoine et des valeurs que partagent les Canadiens et Canadiennes. » (http://www.pch.gc.ca/ccop-pcce/index_f.cfm) Au cours des dix premiers mois de son existence, le site Internet du MVC a fait l'objet de 200 000 visites en moyenne par mois. Le respect des droits de propriété intellectuelle compte parmi les principes du MVC, et les partenaires doivent s'assurer qu'ils détiennent les droits ou qu'ils ont obtenu l'affranchissement des droits sur tous les éléments d'information inclus dans les présentations en ligne.

Le Réseau canadien d'information sur le patrimoine (RCIP) offre un cours, intitulé *Numérisez vos collections*, aux musées qui envisagent de mettre sur pied un projet de numérisation. Ce cours en neuf parties, qui vise à accroître les compétences de la communauté muséale, contient une section intitulée *Considérations juridiques*, qui met l'accent sur les aspects juridiques d'un projet de numérisation et sur le besoin de sécurité relativement à l'affichage et à l'utilisation de contenu numérisé [RCIP, 2000].

Des projets de plus en plus ambitieux de création d'iconothèques en ligne ont fait leur apparition dans les domaines des sciences, des arts et de l'histoire. Le projet Van Eyck décrit sa mission en ces termes :

> « Le projet VAN EYCK vise la création d'un réseau international d'archives photographiques provenant de bibliothèques en histoire de l'art, réseau qui constituerait une ressource unique en son genre pour des fins de recherches et d'études. Pareil réseau pourrait atteindre une masse critique avec la collaboration d'aussi peu que dix des photothèques en histoire de l'art les plus importantes au monde. Cet exercice se trouverait facilité par le nombre relativement restreint de grands centres, notamment la bibliothèque Witt du *Courtauld Institute*, le RKD et le *Marburger Index*, qui détiennent des images, du matériel spécialisé et de l'information pratique sur des millions d'œuvres d'art... » [traduit de *Van Eyck Project*, s. d.]

L'objectif d'avoir des bibliothèques de millions d'images accessibles par Internet n'est pas très lointain. Le projet *American Memory* de la Bibliothèque du Congrès compte (au moment de la rédaction de cet ouvrage) cinq millions d'images numérisées.

Ces développements nous amènent à tirer deux conclusions :

- Le grand public s'attendra, et ce dans une proportion toujours plus grande, à ce que les musées et les services d'archives offrent un accès en direct à un contenu aussi vaste que possible. Les musées qui ne font qu'annoncer leurs expositions ou promouvoir leurs collections sans en révéler quoi que ce soit ne favoriseront pas les visites répétées. On exigera des services d'archives qu'ils maintiennent leur contenu sous une forme qui permette aux

utilisateurs de réseaux de trouver l'information voulue grâce à des outils appropriés comme les moteurs de recherche Web (qui sont pour le moment les outils d'extraction les plus puissants, encore que rudimentaires) ainsi que d'examiner, imprimer, écouter ou utiliser autrement leur contenu.

- Cependant, dans le contexte de la diffusion d'information en direct, les services d'archives numériques devront assumer une responsabilité accrue quant à la gestion des droits de propriété intellectuelle. En effet, ils devront favoriser les transactions entre les détenteurs de droits d'auteur et les usagers, et prendre toutes les précautions raisonnables pour empêcher l'utilisation non autorisée des documents.

2.2 Conservation et images numérisées

La production d'images numérisées d'une résolution toujours plus grande et l'existence de moyens techniques comme *Photo CD* [Smith, 1994], qui permettent de stocker les images qui en résultent de façon à peu près permanente sur cédéroms ou sur DVD produits à peu de frais au musée ou au service d'archives, incitent fortement à la création d'archives numérisées de textes, de manuscrits, de cartes, etc., et rendent caducs certains arguments du passé contre la numérisation [Weber, 1993].

Avec la conservation d'un nombre croissant de documents grâce à ces outils, il faudra prendre soin de respecter les restrictions associées au droit d'auteur.

Les modifications de 1998 à la loi canadienne sur le droit d'auteur précisent en quelles circonstances des images peuvent être copiées (de plus en plus sous forme numérique) à des fins de conservation :

- si l'original est rare ou non publié et doit être conservé,
- pour permettre la consultation sur place si l'original ne peut pas être utilisé en raison de son état ou doit être conservé dans des conditions atmosphériques particulières,
- si l'original est dans un format désuet ou fait appel à une technique non disponible,
- ou si cela est nécessaire à la restauration [Harris, 2000].

2.3 Obligations et risques

Généralement, les musées et les services d'archives sont tenus :

- de protéger la valeur commerciale des images pour lesquelles l'établissement détient le droit d'auteur.

Dans le passé, on menaçait de poursuite judiciaire les personnes qui se rendaient coupables de contrefaçon. Cependant, dans un environnement numérisé en réseau, où les contrefacteurs potentiels sont les utilisateurs ultimes, c'est-à-dire les « visiteurs » du musée, il devient évident que le seul recours aux tribunaux serait inefficace.

- de veiller à ce que l'établissement respecte ses obligations juridiques face aux détenteurs de droit d'auteur pour les images dont il est propriétaire ou pour lesquelles il accorde une licence, sans toutefois être titulaire du droit d'auteur.

Les risques sont réels : un article dans *MUSEUM-L* [Keshet, 1996] décrit une poursuite judiciaire concernant une diapositive couleurs d'une œuvre d'art d'une collection dont est propriétaire un musée, mais pour laquelle l'artiste, maintenant décédé, avait cédé le droit d'auteur à un tiers il y a quelque soixante ans, et ce à l'insu du musée. Le musée se rendait coupable d'un premier délit de contrefaçon en photographiant l'œuvre, et d'un second délit de contrefaçon en offrant l'exploitation sous licence de la diapositive à un éditeur. Malheureusement, la question de savoir qui peut valablement prétendre détenir le droit d'auteur sur une œuvre peut demeurer sans réponse définitive tant que les tribunaux n'en ont pas jugé. À titre d'exemple le rapport des Archives visuelles européennes [EVA, 1999] contient pas moins de cinq opinions divergentes d'experts sur les circonstances dans lesquelles des photographies tombent sous le coup de la loi du Royaume-Uni sur le droit d'auteur et sur qui détient ces droits.

- de s'assurer de l'intégrité et de l'authenticité des reproductions mises à la disposition du grand public, que ce soit par l'établissement ou par des « tierces parties ».

Dans ce cas-ci, le problème est particulièrement aigu, en raison de la facilité avec laquelle on peut copier, manipuler et rediffuser toute information sous forme numérique. Grâce à des logiciels aussi puissants que peu coûteux pour ordinateurs de bureau, pratiquement quiconque ayant des connaissances élémentaires peut reproduire, manipuler et faire imprimer des images, si bien que la contrefaçon devient très aisée et le contrôle très ardu. En outre, les techniques de l'édition moderne exigent que les images soient présentées sous forme numérique de sorte que si, par exemple, une agence de photographie ne fournit que des diapositives, il est presque certain que le client lui-même procédera à la numérisation des images pour les rendre plus faciles à utiliser dans le logiciel d'éditique. La société Kodak elle-même, dans sa publicité sur la technologie de stockage d'images sur *Photo CD*, fonde sa promotion sur le fait qu'il est aisé de manipuler les images :

> « Avec des applications comme *Adobe Photoshop*, vous pouvez modifier les images [sur *Photo CD*] selon vos besoins, quels qu'ils soient. Vous pouvez restaurer d'anciennes photographies, ajouter des personnes sur une photo ou enlever des objets. Et ce n'est qu'un début. » [traduit de l'anglais]

Les musées qui montrent des extraits de leurs collections dans un site Internet ont souvent utilisé des *vignettes* — des reproductions de petite taille et de qualité médiocre, qu'il ne vaut donc pas la peine de copier — afin de contourner le problème de la facilité de la copie et de la rediffusion. Cela présentait aussi un avantage supplémentaire alors que l'espace disque était coûteux et que le téléchargement d'un fichier d'image risquait de prendre beaucoup de temps. Mais les améliorations techniques en matière de numérisation, de stockage et de transmission permettent maintenant d'offrir aux usagers une expérience visuelle de bien meilleure qualité, ce qui hausse d'autant les attentes des usagers. À titre d'exemple, le Musée d'État de l'Hermitage, à Saint-Pétersbourg, en Russie, a utilisé le système *Digital Library* d'IBM pour créer une galerie d'images numérisées entièrement accessibles à grande résolution au moyen d'un navigateur :

> « La décision du Musée de l'Hermitage de rendre toute sa collection accessible à grande résolution — au lieu de n'offrir que quelques images à grande résolution comme le font la

> plupart des musées — est sensée aux yeux de Fred Mintzer, qui dirige le groupe [d'IBM]. 'À première vue, une telle qualité peut sembler superflue, mais elle est en fait nécessaire pour que le visiteur du site Internet puisse commencer à ressentir la beauté de l'art.' » [traduit de Stewart, 1999]

Il est aussi à noter que, dans ce cas, le visiteur virtuel voit les objets numérisés sans avoir à télécharger un logiciel particulier qui pourrait assurer l'application d'un contrat de licence avec le musée.

Dans cette situation, les droits et permissions qui régissent l'accès aux images du Musée de l'Hermitage ne sont pas clairs, mais dans le contexte canadien, une question importante serait celle des droits d'exposition accordés aux créateurs aux termes de la nouvelle *Loi sur le droit d'auteur* (RSC 1985, c.C-42, telle qu'amendée) de 1988 [Rottenberg, 1997]. Il est probable que toute présentation dans un réseau public de l'image numérique d'une œuvre produite après 1988 sera interprétée comme une « exposition », si bien qu'il sera nécessaire d'obtenir l'autorisation du titulaire du droit d'auteur.

Greg Spurgeon, du Musée des beaux-arts du Canada, a fait remarquer que ce droit d'exposition...

> « met en opposition la volonté qu'ont la plupart des musées d'art de soutenir les droits moraux et économiques des créateurs d'une part, et leur capacité de promouvoir et d'exposer l'art contemporain en raison de ces nouvelles obligations financières et administratives d'autre part. Certains ont créé les mécanismes nécessaires pour négocier et payer les frais d'exposition (bien qu'il s'agisse là d'un fardeau administratif de plus en plus lourd, et ce à une époque de compressions généralisées dans les musées). D'autres continuent de chercher des moyens d'exploiter sous licence les expositions et d'obtenir d'autres droits dans l'optique du respect des droits du créateur ou du titulaire du droit d'auteur sans imposer au musée un fardeau qui le gênerait dans la réalisation des programmes de son mandat. » [traduit de *MUSEUM-L*, 11 avril 1996]

2.4 L'exploitation sous licence : un moyen de sensibilisation

Les gens tiennent souvent pour acquis qu'ils ont le droit de copier, de faire imprimer et de diffuser tout ce qu'ils trouvent dans Internet. On justifie souvent l'existence supposée de ce droit par le fait que de nombreux outils que nous employons pour le courriel, les forums de discussion, ou pour aller chercher un document par FTP, ainsi que la plus grande partie de l'information elle-même, ont été créés de façon désintéressée. Il n'est pas rare de voir des documents dans le Web ou dans un répertoire FTP accompagnés d'un avis disant qu'ils sont rendus accessibles « dans l'esprit de partage d'information par Internet ».

Dans cet esprit, l'initiative américaine sans but lucratif *Internet Moving Images Archive*, qui rassemble des documents numérisés portant sur l'histoire sociale des États-Unis au XX^{e} siècle, a mis dans son site Web son catalogue vidéo de plus de 1 000 titres. Ces fichiers sont disponibles gratuitement et sans restriction, mis à part que « les films ne peuvent être revendus ou exploités sous licence par quiconque, que ce soit en tout ou en partie. » [traduit de *Internet Archive*, 2001].

Malgré la commercialisation d'Internet, il y a toujours des ressources du domaine public. Certaines institutions américaines, notamment la NASA, mettent à la disposition des internautes de vastes collections d'images scientifiques et historiques, et ce sans restriction aucune. Citons à titre d'exemple la *Dryden Research Aircraft Photo Archive*, qui contient des photos numérisées d'images d'aéronefs de recherche datant des années 1940 jusqu'à aujourd'hui, et pour lesquelles il est *explicitement mentionné* qu'aucune protection du droit d'auteur n'est mise en œuvre. Dans le cas de la collection *American Memory* de la Bibliothèque du Congrès, la bibliothèque fournit des renseignements sur les détenteurs du droit d'auteur et les restrictions qui s'appliquent, tout en laissant à l'usager le soin de déterminer quelles utilisations des images sont appropriées.

Dans le monde de l'édition de logiciels, nous nous sommes habitués au fait que le client et l'éditeur doivent passer un contrat. Comme Strong [1994] le fait remarquer :

> « Cela n'a jamais été le cas auparavant. La transaction typique entre l'éditeur et le client se déroulait dans une librairie où le client payait et ressortait du commerce avec ce qu'il avait acheté. À mesure que les liens entre l'éditeur et le client vont se resserrer, les rapports seront ou bien plus hostiles, ou bien plus interactifs et instructifs pour l'une et l'autre parties. » [traduit de l'anglais]

Howard Knopf, avocat canadien expert du droit d'auteur [Norman, 1995], prévoit un ressac si le principe de l'utilisation équitable est éliminé ou considérablement restreint. « Les lois doivent persuader et non menacer [...] Trop protéger le droit d'auteur pourrait bien avoir pour effet d'arrêter la construction de l'inforoute. » [traduit de l'anglais] Cette question est devenue particulièrement controversée dans le cas de la diffusion numérique de musique populaire en vertu des clauses, définies par l'industrie, de la *Digital Millennium Act* des États-Unis. On a notamment fait valoir que

> « les propriétaires de contenu et les entreprises de gestion numérique des droits découragent la croissance de la musique numérique en contrôlant à leur guise les droits d'auteur. » [traduit de King, 2001]

Des critiques tels que le professeur Edward Felton, de l'université Princeton, affirment que, au lieu de mettre l'accent sur la mise en œuvre de moyens commodes de paiement et sur le développement d'applications de détection du piratage, les principales entreprises qui offrent du contenu se sont efforcées d'acquérir « un contrôle sans précédent sur le droit d'auteur » lui-même afin de bloquer des droits que les usagers avaient auparavant.

Par contre, les diffuseurs d'images sont de plus en plus nombreux à établir des liens vers de l'information en direct sur le droit d'auteur et la loi sur le droit d'auteur, à l'intention des usagers qui désirent obtenir de plus amples renseignements. Il est possible de faire beaucoup plus en ce sens grâce à l'interactivité puissante des serveurs et des navigateurs Web. Ainsi, les fournisseurs sont en mesure d'expliquer la nature et l'objet du droit d'auteur et de sensibiliser les usagers à cette question.

À titre d'exemple, la *Bridgeman Art Library*, important diffuseur commercial d'images au Royaume-Uni, met en bonne place, dans la barre de navigation principale de son site Internet, les renseignements relatifs au droit d'auteur en ce qui a trait à l'utilisation de ces images. Ce lien

amène l'usager directement vers une liste d'articles récents sur le droit d'auteur et les images dans le Web, puis vers une page où l'usager peut choisir l'utilisation prévue des images : académique, personnelle, éditoriale ou commerciale. Une fois le type d'utilisation choisi, le système affiche une explication détaillée des responsabilités de l'usager [Bridgeman, 1999].

La bibliothèque du consortium AMICO (*Art Museum Image Consortium*) à l'Université de l'Alberta explique les conditions d'utilisation des images dans la page qui donne accès à la base de données :

> « L'accès et l'utilisation de la bibliothèque AMICO sont réservés exclusivement à des fins d'enseignement, de recherche et de travaux savants... La bibliothèque AMICO peut être utilisée pour (1) l'enseignement en classe et des activités connexes, (2) les devoirs des étudiants, (3) l'exposition publique dans le musée d'une université ou une installation semblable,... (4) l'exposition publique... dans le cadre d'une présentation professionnelle,... (5) le portfolio d'un étudiant ou d'un professeur,... et (6) une thèse ... » [traduit de Université de l'Alberta, s. d.].

Il est intéressant de noter que non seulement les restrictions que les usagers devraient connaître sont mentionnées, mais aussi des situations d'utilisation qui correspondent à leurs besoins.

Dans le cadre des Collections numérisées de Rescol, le site Internet de Parcs Canada contient une galerie d'images destinée aux élèves. Les renseignements sur l'utilisation des images sont donnés dans un style simple à la portée des enfants. La page d'accueil contient un lien vers une explication de la manière dont les élèves peuvent utiliser les images :

> « Les images que vous trouverez ici proviennent d'une vaste collection appartenant à Parcs Canada. Vous pouvez les télécharger, les sauvegarder et les imprimer pour vos projets scolaires ou simplement parce qu'elles vous plaisent! »

L'explication comporte aussi une section sur la définition du droit d'auteur tel qu'il s'applique aux images de cette galerie :

> « Que signifie © Parcs Canada? Cela signifie simplement que chacune des illustrations incluses dans 'Images de Parcs Canada' appartient à Parcs Canada. Vous pouvez télécharger ces illustrations, les sauvegarder et les imprimer pour vos travaux scolaires » [traduit de Parcs Canada, s. d.]

L'avis de droit d'auteur du site Internet du *Musée virtuel du Canada* résume les utilisations autorisées du contenu du site :

> « **Droit d'auteur**
> Sauf indication contraire, tout le matériel de ce site Web, notamment les images, les illustrations, les concepts, les icônes, les photographies, les clips vidéo, les textes et autres éléments sont protégés par des droits d'auteur, marques, concepts exclusifs et (ou) d'autres formes de propriété intellectuelle appartenant au Réseau canadien d'information sur le patrimoine (RCIP) ou à ses musées membres, ou contrôlées ou exploitées sous licence par eux.
> Nous vous invitons à utiliser le matériel du site Web du MVC à des fins éducatives ou personnelles. Le cas échéant, les avis de droit d'auteur et autres avis de propriété devraient être conservés avec les éléments de matériel auxquels ils se rapportent.
> Pour toutes autres fins, notamment pour des fins commerciales, on ne peut, sans

> l'autorisation expresse du RCIP et, s'il y a lieu, des autres titulaires des droits d'auteur, modifier, copier, reproduire, republier, afficher, transmettre ou distribuer tout ou partie du matériel du site Web du MVC de quelque manière que ce soit. »

Dans le cas de matériel numérique, les licences d'accès contrôlent souvent davantage que les lois sur le droit d'auteur les conditions d'utilisation. Dans les milieux universitaires, l'exploitation sous licence pour procurer un accès protégé et restreint aux documents d'archives est devenue très controversée, car on considère qu'elle mine le droit traditionnel à un « usage loyal » (le *fair use* dans la loi américaine sur le droit d'auteur) et à la copie pour des fins d'érudition. Ce n'est pas le cas de licences conçues en fonction des usagers, par exemple celles d'AMICO, qui disent explicitement ne pas limiter l'« usage loyal » et permettent même des utilisations qui vont au-delà [AMICO, Foire aux questions, s. d.]. Mais, de manière générale, « l'exploitation sous licence coupe l'usage loyal » [traduit de Snow, 1997], comme le montre de manière très évidente un effet des clauses fort controversées du *Digital Millennium Copyright Act* aux États-Unis, en vigueur depuis octobre 2000 :

> « en criminalisant le contournement d'un système technique de protection mis en place par le détenteur du droit d'auteur — même si quelqu'un a le droit d'accéder à cette information en vertu du principe de l'usage loyal... Par conséquent, le public [des États-Unis] aura moins de droits dans le domaine numérique que dans le contexte traditionnel en matière d'utilisation et d'accès à l'information. » [traduit de Gross, 2000]

Le commentaire suivant émis par l'*American Library Association* illustre l'inquiétude que cela suscite au sein des bibliothèques et des institutions d'enseignement en général :

> « À long terme, ces 'verrous technologiques' pourraient avoir un impact énorme sur la capacité des bibliothèques d'offrir l'accès à des documents, de les prêter et de les archiver, ainsi que sur la capacité des usagers des bibliothèques d'utiliser pleinement ces ressources. » [traduit de ALA, 2001]

D'autre part, il se peut que les musées ne puissent pas revendiquer le droit d'auteur sur des images numériques d'œuvres d'art du domaine public, précisément parce que ces images ne font que reproduire des objets et ne contiennent donc pas l'élément d'originalité requis pour créer une œuvre protégée par le droit d'auteur! C'est la conclusion d'un jugement prononcé en 1999 aux États-Unis contre la *Bridgeman Art Library* (en vertu toutefois de la loi britannique sur le droit d'auteur) et en faveur de Corel Corporation à propos d'un cédérom contenant des reproductions numériques de tableaux bien connus de maîtres européens, dont 120 œuvres d'art sur lesquelles Bridgeman prétendait avoir le contrôle exclusif. Les implications de ce jugement pour les musées sont décrites par Barry G. Szczesny, conseillers aux affaires gouvernementales de l'*American Association of Museums* :

> « Le cas Bridgeman soulève des inquiétudes pour des projets tels que ceux de la MDLC (*Museum Digital Library Collection*) et d'AMICO (*Art Museum Image Consortium*)... Un avis juridique à propos des options possibles pour la protection juridique des images numériques d'œuvres du domaine public suite au cas Bridgeman recommande une combinaison des éléments suivants :
>
> 1. Introduire des éléments de création dans le processus de numérisation afin d'augmenter la probabilité que les copies numériques puissent être protégées par le droit d'auteur (mais cela irait à l'encontre de l'objectif de fournir une véritable reproduction).

2. Rassembler des images numérisées dans une collection peut permettre d'accorder à la collection dans son ensemble une protection en vertu du droit d'auteur, tout comme le feraient des textes ou de la documentation à valeur ajoutée, mais cela ne protège pas les œuvres elles-mêmes si elles ne sont pas protégées indépendamment.
3. Tenter d'imposer des restrictions contractuelles sur l'utilisation subséquente des copies numériques dans le cadre d'un contrat de licence (mais il faut noter qu'un tel contrat ne lie pas une tierce partie qui obtient l'image numérique).
4. Explorer la possibilité de restreindre la copie par des moyens techniques. C'est la mesure la plus pratique.

Ce qui sera peut-être le plus important pour les musées sera de mieux éduquer le public dans le domaine des droits et des reproductions. » [traduit de Szczesny, 1999]

Le jugement dans le cas Bridgeman pourrait aussi avoir des conséquences sur les modalités de licence d'accès aux collections d'images numériques des universités. Un accès restreint à un réseau précis, comme le montre l'avis ci-dessous de la banque d'images Dido de l'Université de l'Indiana :

Pas d'accès

Pour des raisons de droit d'auteur, les images de la banque d'images Dido ne sont accessibles qu'à partir du réseau du campus Bloomington de l'Université de l'Indiana.

aurait une certaine efficacité, mais si un professeur de cette université faisait des copies d'images de la banque Dido et les distribuait à ses étudiants, il semble que cela ne constituerait pas une violation du droit d'auteur (voir le point 3 ci-dessus.)

Les conséquences de ces questions sur la jurisprudence canadienne ou sur les modifications à venir à la loi canadienne sur le droit d'auteur sont incertaines. Quoi qu'il en soit, des modifications à la loi sont déjà nécessaires pour aller au-delà de la notion restreinte de « reproduction par reprographie » (avec balayage numérique, par exemple dans un photocopieur, mais seulement sur papier et non vers un fichier informatique) et couvrir des œuvres enregistrées et copiées sous forme numérique.

2.5 La normalisation des contrats de licence

La mise au point de contrats normalisés de licence, qui reflètent un consensus quant à des « pratiques acceptables » réalistes constitue un progrès important permettant aux musées de mieux remplir leur mandat de diffusion tout en protégeant la propriété intellectuelle. [RCIP, 1997]. Le projet AMICO de l'*Association of Art Museum Directors* a contribué de manière importante à cet effort en définissant un cadre détaillé des droits, permissions et restrictions d'utilisation en matière d'images numérisées. [AMICO, 1998] Comme un grand nombre des « clients » d'un accès élargi au contenu muséal sous forme numérique sont des institutions d'enseignement, il semble probable que les musées ressentiront les effets de la tendance de ces institutions à former des consortiums qui, grâce à des contrats de licence à grande portée, obtiendront des conditions d'utilisation et de coût plus favorables que sur une base individuelle. Un exemple remarquable est celui du Projet canadien de licences de site nationales (PCLSN) [Schofield, 2000], qui porte surtout sur des revues électroniques et bases de données de recherche plein texte, principalement dans les

domaines des sciences, de la technologie et des disciplines médicales. Cette expérience peut, du moins dans une certaine mesure, être appliquée par les universités et collèges à la négociation de licences de site avec des musées et des associations de musées au Canada.

Il y a clairement une évolution dans le choix entre l'exploitation sous licence et la vente. Le Projet de numérisation des collections du Musée canadien des civilisations, lancé en 1993, visait initialement la vente des images numérisées. Mais d'après l'expérience du Musée, l'exploitation sous licence constitue une meilleure utilisation de la ressource. Sur une banque de plus de 300 000 images numériques,

> « moins de 1 000 ont été vendues comme on le projetait à l'origine, mais davantage ont fait l'objet de licences d'utilisation. » [traduit de Tomlin, 2000]

L'élaboration d'accords de licence standard ne suffira pas à elle seule à rendre généralement réalisables en pratique l'exposition et la diffusion d'images numériques. Les musées auront également besoin de systèmes informatiques de gestion, comportant une base de données, capables d'enregistrer de manière continue les centaines et les milliers de contrats de licence susceptibles de régir dans l'avenir les images d'œuvres protégées par le droit d'auteur. Ces systèmes informatiques, que l'on appelle *systèmes de gestion des droits d'auteur*, font l'objet du chapitre qui suit.

3 Systèmes de gestion numérique des droits d'auteur

Un certain nombre de techniques nouvelles peuvent réduire le besoin de dispositions improductives ou trop rigides : ce sont les *systèmes de gestion numérique des droits d'auteur* (ou SGDN pour systèmes de gestion des droits numériques), c'est-à-dire des bases de données en réseau et accessibles à distance qui contiennent des données sur les usagers, les auteurs, les licences et l'utilisation, et qui ont pour objet de limiter et de permettre l'accès des usagers à l'information qui circule dans un réseau. Ces systèmes permettent de réduire considérablement les frais liés aux transactions et aux contrats de licence. Grâce à eux, il est beaucoup plus facile de facturer et de percevoir des frais raisonnables pour une information à valeur commerciale, tout en donnant la possibilité aux fournisseurs d'offrir un accès à une information autre sans frais ou pour un prix symbolique. Ceci devrait permettre aux musées (et aux autres fournisseurs de produits multimédias éducatifs) d'acquérir facilement les droits de présentation ou d'exposition d'images et d'autres médias. [Hoffert, 1996]

Les systèmes de gestion des droits d'auteur présents dans les institutions d'enseignement et applicables au contexte d'un musée trouvent leurs fondements dans les *serveurs de licences*, c'est-à-dire des logiciels de gestion de système qui tiennent le compte du nombre de copies de logiciel exploitées sous licence dans un laboratoire ou un réseau local. De tels systèmes ne conviennent pas au traitement des exigences complexes en matière d'exploitation sous licence et de production de rapports qui caractérisent la diffusion en ligne de matériel de plusieurs éditeurs de contenu dans une variété de conditions d'utilisation. Pour cette raison, les logiciels de SGDN sont devenus des produits complexes et multifonctionnels, comme le montrent les exemples donnés plus loin dans ce chapitre. Ces logiciels sont donc susceptibles d'être installés et exploités de manière centralisée à l'échelle de l'établissement plutôt que dans un laboratoire ou un service en particulier.

3.1 Conteneurs et superdiffusion

Les systèmes de gestion des droits d'auteur doivent pouvoir convaincre les propriétaires que leurs biens sont protégés et qu'ils ne seront pas rediffusés. Il n'existait jusqu'à récemment aucun moyen pratique d'y parvenir. Comme le soulignait Harland Cleveland [1985], toute information présentant une certaine valeur est par le fait même une occasion de délit, d'autant plus que le coût lié à ce délit (la copie) tend à être nul. Mais ce n'est plus le cas si l'information est encapsulée dans un « conteneur » logiciel étanche (chiffré) qui permet une copie gratuite, mais qui exige une opération (autorisation, inscription, reconnaissance de dette, etc.) avant tout accès à son contenu.

Ces conteneurs permettent par ailleurs ce que l'on appelle la *superdiffusion* [Cox, B., 1996]. Ils agissent comme vecteurs d'une information qui peut être copiée gratuitement et rediffusée sans préjudice économique pour les titulaires de droits d'auteur — en fait, la copie représente même un *avantage* économique pour eux puisqu'il est ainsi possible pour un nombre plus important d'usagers d'acquérir le conteneur, de se conformer aux conditions de la licence, dont le versement de droits, et d'avoir accès au contenu. (Aussi ironique que cela puisse paraître, les licences de superdiffusion devront *exonérer* l'usager du délit de contrefaçon lorsqu'il copiera le conteneur pour des fins de rediffusion.)

Un musée, par exemple, pourra monter une exposition à partir de nombreux éléments interactifs, dont des images, utilisées sous licence, d'objets appartenant à d'autres musées ou lui appartenant en propre, des documents textuels protégés par le droit d'auteur, des documents sonores dont les droits d'exécution appartiennent au compositeur, etc. Tous ces éléments pourront être acquis par le musée (vraisemblablement au moyen d'Internet) grâce à des conteneurs chiffrés. Le musée utilisera alors les outils logiciels appropriés pour réunir son matériel (également mis en conteneur) en une seule présentation ou application interactive, qu'il diffusera alors gratuitement aux consommateurs (« visiteurs virtuels ») par Internet pour une période donnée. Le musée se trouvera donc à diffuser son propre matériel et à rediffuser le matériel d'autres musées, et ce à peu de frais.

Les utilisateurs du produit du musée auront des interactions par Internet avec un système de gestion des droits d'auteur ou un système de gestion de la propriété intellectuelle qui se chargera des licences, du paiement, etc., non seulement pour le conteneur externe créé par le musée, mais aussi pour tous les sous-conteneurs obtenus d'autres sources. Ces sources pourront aussi toucher des redevances sans que leur musée ait à participer directement au transfert des droits, des permissions ou des fonds.

3.2 Systèmes de gestion des droits d'auteur

Pour donner une idée de ce que les fournisseurs de contenu comme les musées peuvent attendre des systèmes de gestion des droits d'auteur, nous aborderons brièvement les caractéristiques générales présentes dans tous les grands systèmes adaptés à la diffusion d'images ou, de manière plus générale, de documents multimédias, puis nous examinerons plusieurs systèmes précis actuellement disponibles ou en cours de développement :

- ContentGuard,
- *l'environnement de diffusion virtuelle* InterTrust,
- RightsMarket,
- OnDisC.

Caractéristiques générales

- *Contrôle de l'accès* — L'accès est contrôlé au moyen d'un registre qui contient le justificatif d'identité et le profil des usagers. Ce registre vise à faire une « évaluation de la permission d'accès » qui détermine le droit de l'usager d'accéder à des sources d'information données.

- *Authentification* — Cette fonction sert à confirmer l'identité de l'usager. Pour la plupart des opérations dans Internet, l'authentification utilise actuellement un code et un mot de passe attribués à l'usager au moment de son inscription. Cependant, l'authentification à des fins de commerce électronique fera de plus en plus appel à des identificateurs numériques infalsifiables, ou certificats, pour confirmer l'identité de l'usager et de ses affiliations.

L'authentification s'applique aussi au serveur de documents du fournisseur d'information (par exemple, le serveur Web d'un musée) lorsque ce serveur demande d'accéder au système de

gestion des droits d'auteur, afin d'éviter le problème posé lorsqu'un serveur relié à Internet est programmé pour s'identifier comme étant un autre serveur.

- *Navigateurs* — Toutes les opérations sont transmises dans Internet par HTTP (*Hypertext Transfer Protocol* ou protocole de transfert hypertexte) [Berners-Lee, 1994]. Les opérations protégées entre le navigateur et les serveurs font appel à des fonctions de sécurité à base de chiffrage intégrées dans les navigateurs, par exemple *Netscape Navigator/Communicator*, qui reconnaissent le protocole SSL (*Secure Sockets Layer*).

Les fonctions d'un logiciel de navigation peuvent être étendues par l'ajout de modules supplémentaires, appelés plugiciels, que l'usager peut télédécharger dans son ordinateur à partir d'Internet. Un module de gestion des droits d'auteur peut servir à traiter une demande émise par un client et extraire un document déchiffré de son conteneur chiffré afin de le rendre accessible au logiciel de navigation. (Le chiffrage et la technique du conteneur sont présentés en détail au chapitre 4.)

- *Applications personnalisées* — Un fournisseur ou diffuseur de contenu protégé peut vouloir fournir à l'usager une interface particulière qui remplace le navigateur. Pour éviter que ces applications ne dépendent du matériel et du système d'exploitation de l'usager, on utilise le langage Java, largement répandu, pour les écrire sous forme d'*applets* automatiquement télédéchargés à partir d'Internet lorsqu'on en a besoin, et qui disparaissent du système de l'usager une fois terminés. Une caractéristique importante des applets est leur capacité de contrôler les opérations (p. ex., impression, enregistrement) que l'usager peut effectuer sur le contenu protégé, en fonction de sa licence d'utilisation ou des permissions d'accès qui lui sont accordées.

- *Centre de compensation* — Lorsqu'il atteint une certaine taille, un système de gestion des droits d'auteur requiert un centre de compensation qui produit des registres de l'utilisation, des paiements, des licences accordées et du nouveau contenu.

- *Identification* — Dans le cas de contenu multimédia, une forme de protection qui gagne en importance consiste à incorporer dans le contenu, sous forme de *filigranes* visibles ou non, l'identification de la source —auteur ou éditeur— (voir la section 4.1). L'information de diffusion, qui comprend l'identification de l'usager, peut également être dissimulée dans la copie d'un document transmis à un usager afin d'empêcher toute redifíusion non autorisée.

3.2.1 *ContentGuard*

ContentGuard[MC] est un exemple du genre de produit de gestion numérique des ressources disponible sur le marché pour des organismes qui souhaitent exercer un contrôle très détaillé de l'utilisation de leur contenu. L'établissement propriétaire du contenu définit une politique concernant l'utilisation dans son sens le plus large de l'information numérisée. À l'aide de métadonnées codées dans le langage de définition XrML[MC] (voir la section 5.1), le propriétaire du

contenu peut préciser les droits accordés à l'usager et les conditions dans lesquelles ces droits sont accordés. Ces métadonnées, qui constituent une « étiquette des droits », comportent toutes les conditions d'utilisation du contenu, notamment les frais d'accès et la durée d'utilisation. Elles contiennent également une description sommaire du contenu et servent à créer la licence émise à l'usager. Le propriétaire du contenu exerce un contrôle entier et personnalisé sur la capacité de l'usager à faire imprimer ou afficher, enregistrer, modifier, copier ou rediffuser le contenu.

Cette approche de la gestion à large spectre du contenu met en œuvre une forme de superdiffusion protégée, puisque lorsqu'un contenu accompagné d'une étiquette des droits est envoyé par courriel ou diffusé d'une autre manière par un usager qui détient une licence vers un usager qui n'en détient pas, l'accès au contenu est refusé. L'usager qui n'a pas de licence est orienté vers le site Internet du propriétaire du contenu afin d'obtenir un accès autorisé. Dans le jargon de *ContentGuard*, ce processus s'appelle la « mise en application persistante des droits ».

ContentGuard protège actuellement des documents textuels (p. ex des fichiers en HTML, XML, Quark, PDF, Word et Excel). Des produits semblables pour la protection de documents audio et vidéo sont en cours de réalisation.

3.2.2 *InterTrust*

InterTrust Technologies a fait breveter un certain nombre d'inventions portant sur la mesure de quantités d'information, la sécurité de données décentralisées, la superdiffusion et la protection des droits numériques, le tout constituant la base de ce qui est appelé « technologie *InterTrust Virtual Distribution Environment*[MC] (environnement de diffusion virtuelle *InterTrust*) pour répondre aux besoins critiques, mais non satisfaits, du commerce électronique ». Au lieu d'offrir un produit ou un système, *InterTrust* propose un ensemble d'outils à l'intention des réalisateurs d'applications de gestion des droits d'auteur.

InterTrust fait appel à la technique des conteneurs pour assurer la sécurité de l'information à diffuser et pour s'assurer que l'information est bel et bien utilisée conformément aux règles et aux contrôles qui précisent les usages permis ainsi que les répercussions de l'utilisation. Mais contrairement à IBM, InterTrust Technologies a choisi de ne pas confier la diffusion de contenu à des serveurs centraux. Au lieu de cela, des systèmes indépendants échangent des droits, des licences, des clés d'accès, etc., ainsi que des documents, à l'aide de conteneurs logiciels étanches appelés *DigiBox*[MC] (voir le paragraphe 4.4.1).

La technologie d'*InterTrust* incorpore ses procédures directement dans le système d'exploitation de l'ordinateur, ou encore vient enrichir le système, afin de créer un environnement d'exploitation protégé appelé *InterTrust Commerce Node* (nœud de commerce *InterTrust*). Il est probable que, dans un avenir rapproché, il ne sera plus nécessaire de procéder ainsi puisque les systèmes d'exploitation sont de plus en plus *modulaires* — c'est-à-dire faits de petits éléments logiciels réutilisables qui, de manière indépendante, peuvent assurer l'accès aux applications et aux ressources du système d'exploitation.

Une architecture modulaire va de pair avec les conteneurs logiciels et, comme le montre *InterTrust*, les conteneurs logiciels étanches sont probablement appelés à jouer un rôle important dans le domaine de la superdiffusion.

3.2.3 *RightsMarket*

RightsMarket (présenté plus en détail au paragraphe 4.4.2) est un produit canadien dans le domaine de la gestion des droits d'auteur. Ce système crée un certain nombre de bases de données qui servent à la gestion des droits d'auteur :

- contrats entre consommateurs et éditeurs ou diffuseurs qui exploitent le logiciel *RightsMarket*,
- données de facturation (tenues à jour dans l'ordinateur du client et dans celui du distributeur),
- liste des objets (numériques) qui peuvent être diffusés.

RightsMarket requiert l'installation d'une application *Windows* dans l'ordinateur de l'usager.

La diffusion d'objets peut se faire de différentes manières, par exemple par Internet à l'aide d'un nagivateur ordinaire ou sur un support physique tel qu'un disque optique compact. Les objets sont traités par un « module d'emballage » *RightsMarket*, qui les encapsule de telle sorte que l'usager doit avoir un module de visualisation autorisé pour pouvoir ouvrir et utiliser le contenu. Comme dans le cas de *ContentGuard*, la technologie de *RightsMarket* permet une superdiffusion protégée.

Dans la version actuelle du système, le contenu protégé doit être diffusé à partir d'un serveur géré par *RightsMarket*. *RightsMarket* contrôle également la base de données des usagers et de l'utilisation des objets, et s'en sert pour authentifier les usagers qui ont une licence et pour produire des rapports comptables à l'intention des fournisseurs de contenu.

3.2.4 *OnDisC*

Le groupe de recherche *OnDisC*, qui rassemble des propriétaires de contenu numérique et des institutions d'enseignement postsecondaire, travaille à la mise au point d'outils de gestion de la diffusion de contenu numérique multimédia à des fins éducatives. Le prototype du projet consiste en des « trousses éducatives » de contenu numérique destinées à être distribuées aux étudiants. Ce projet, dont le siège est situé au collège Sheridan, à Oakville, en Ontario, fera d'abord l'objet de tests dans des institutions d'enseignement de l'Ontario, puis sera étendu à tout le Canada dans le cadre du réseau à grand débit CANARIE pour l'éducation et la recherche.

Le projet *OnDisC* se veut un modèle de construction d'un « catalogue collectif » de contenu numérique, avec gestion intégrée des droits correspondants et suivi de l'utilisation. Le contenu provient d'une variété de fournisseurs et est destiné à être diffusé à des professeurs et à des étudiants dans diverses institutions d'enseignement postsecondaire.

Dans le système *OnDisC*, les professeurs créent des « trousses éducatives » en choisissant du contenu numérique dans le catalogue disponible au sein de leur institution. Le contenu est diffusé à partir d'une base de données selon les exigences de son propriétaire. La diffusion peut se faire en ligne sans possibilité de copie, ou dans un format hors ligne, qui permet de faire une copie sur papier ou d'enregistrer une copie personnelle dans un fichier pour l'utiliser ultérieurement. Un registre d'utilisation est remis aux propriétaires de contenu et aux institutions participantes.

Les institutions d'enseignement peuvent fournir aussi bien qu'utiliser du contenu, mais les fournisseurs de contenu sont généralement des producteurs de médias numériques, notamment des éditeurs, des services d'archives (p. ex., le Centre de musique canadienne) et des musées. Une importante source de contenu pour le prototype de *OnDisC* est la base de données d'images accessible par l'intermédiaire du Réseau canadien d'information sur le patrimoine. En plus d'images, les types de média testés dans le prototype comprennent des partitions musicales, des séquences vidéo, de la musique enregistrée, des photographies, des animations, des simulations, des graphiques, des cédéroms et, bien entendu, des textes.

L'accès à *OnDisC* est régi par des licences semblables à celles employées par AMICO ou à celles proposées par le Projet canadien de licences de site nationales mentionné à la section 2.5. Ces contrats de licence de diffusion de contenu numérique offrent aux propriétaires comme aux usagers plus de souplesse que des contrats de vente portant sur des articles individuels. Les conditions de licence peuvent être moins onéreuses pour les usagers et mieux adaptées à des besoins éducatifs, alors que les propriétaires de contenu tirent des revenus de leur propriété intellectuelle et contrôlent l'utilisation du contenu.

Le but du projet *OnDisC* est de démontrer que la technologie actuellement disponible permet de produire un système de diffusion ouvert qui combine :

- la création et la gestion d'une description du contenu (les catalogues),
- une diffusion protégée à des usagers qui ont une licence de site,
- l'intégration à un système de gestion des droits d'auteur afin de procurer aux fournisseurs de contenu des données comptables et d'utilisation.

3.3 La technologie de diffusion comme moyen de protéger les droits de propriété intellectuelle

Les modes traditionnels de diffusion de contenu par Internet supposent le transfert d'un fichier d'un ordinateur à un autre, que ce soit par le bon vieux service *ftp*, ou maintenant par un serveur *http* (serveur Web) où chaque fichier est une page Web ou un élément d'une page Web. Dans un cas comme dans l'autre, le contenu est enregistré dans l'ordinateur récepteur sous forme de copies de fichiers.

Le principal problème, du point de vue de la protection et de la gestion des droits de propriété intellectuelle associés à un contenu numérique accessible par réseau, vient de l'existence de ces

copies. Une fois que le contenu est disponible sous forme de fichier dans l'ordinateur de l'usager, il est évident qu'il n'y a plus vraiment de restrictions sur ce que l'usager peut faire de cette suite de signaux binaires. Même si le contenu est chiffré, il demeure toujours possible de le copier, de le transférer et de l'examiner en tant que fichier de données.

Il existe toutefois des modes de diffusion de contenus qui atténuent considérablement ce problème, en utilisant un protocole réseau par lequel le système d'exploitation de l'usager traite une partie du système de fichiers du serveur comme s'il faisait partie du système de fichiers local (en lecture seule, bien entendu), de telle sorte que les fichiers stockés dans le serveur peuvent être ouverts à distance sans être copiés dans un disque local (puisque le système de l'usager les considère déjà comme des fichiers locaux). C'est ce que l'on appelle le « montage à distance ». Combinée à un système de gestion des droits d'auteur qui contrôle l'accès aux fichiers du serveur, cette technique protège les droits de propriété intellectuelle en supprimant le transfert physique de documents vers le disque de l'usager.

Les applications conviennent évidemment très bien à ce genre d'appel à distance puisqu'elles s'exécutent en mémoire vive et ne laissent normalement pas de copie sur disque sous une forme qui puisse être facilement récupérée. Les fichiers audio et vidéo en continu sont également bien adaptés à ce genre de protection car un logiciel spécial (en général un plugiciel) doit être exécuté dans l'ordinateur de l'usager pour traiter la séquence de données. De plus, les fichiers ainsi transmis sont souvent beaucoup trop volumineux pour pouvoir être commodément enregistrés dans le disque de l'usager.
Mais qu'en est-il des *images*? Elles ne sont ni exécutées ni mises en continu. Si l'on utilise des logiciels de navigation ou d'infographie traditionnels pour les ouvrir, même à distance, les images demeurent vulnérables aux transgressions habituelles de la part de l'usager. La solution consiste à ne les rendre accessibles à distance que par l'intermédiaire d'une application spéciale, d'un plugiciel ou d'un applet qui affiche l'image tout en contrôlant ou en limitant l'impression et la copie. Cela n'empêche pas complètement de faire des copies locales des fichiers à distance, mais cela élimine les possibilités de copie et de rediffusion fortuites qui inquiètent tant les musées et les services d'archives.

3.3.1 Alchemedia *et* Vyoufirst

Des systèmes de gestion des droits d'auteur dotés de fonction plus simples que les systèmes complets décrits plus haut sont également offerts dans le commerce. Ces systèmes sont conçus spécialement pour la protection d'images (typiquement dans les formats JPEG, GIF et PDF). Un exemple représentatif de ces systèmes est *Alchemedia* qui comporte :

- un module de chiffrage qui interagit avec le serveur Internet du fournisseur pour chiffrer les fichiers demandés avant leur transmission vers le navigateur d'un usager,

- un module de visualisation propre à ce système, qui agit comme application auxiliaire du navigateur pour permettre le visionnement des fichiers chiffrés et appliquer les restrictions d'utilisation,

- un outil de gestion à distance qui permet au fournisseur de contenu de définir le module de configuration de son site Internet.

Un autre produit semblable est *Vyoufirst*[MC] de la société Vyou inc., qui exige toutefois de la part du fournisseur de contenu l'installation d'un serveur Web spécial pour diffuser le contenu chiffré. Vyou affirme procurer une vaste gamme de fonctions de contrôle de l'utilisation du contenu, notamment :

- le blocage de la mise en antémémoire (création de copies temporaires sur disque),
- l'impossibilité d'utiliser des débogueurs (qui accèdent directement à la mémoire vive) pour saisir le contenu transmis,
- le blocage des opérations du Presse-papiers, y compris celles de logiciels de tierces parties qui peuvent fonctionner indépendamment des fonctions intégrées au système d'exploitation,
- le blocage des opérations de saisie d'écran.

Le problème de telles prétentions est qu'il est très difficile d'évaluer jusqu'à quel point les contrôles annoncés sont effectifs dans la pratique. Pour déterminer le degré de protection offert par un produit, il faudrait connaître les mécanismes employés. Mais cela est précisément le secret que les fournisseurs de systèmes de sécurité doivent jalousement garder pour éviter que les failles de leurs produits soient connues et publicisées par les « exploits » d'un pirate. Le chiffrage, qui constitue la technologie fondamentale de ces produits, peut prévenir la violation fortuite tout comme les mots de passe et les codes d'accès. Mais il est loin de constituer la protection ultime de documents précieux, comme le montre la grande disponibilité de logiciels capables de percer le chiffrage de films commerciaux en format DVD. (Un sondage informel mené dans un groupe d'étudiants en informatique à l'université a montré que près de la moitié des étudiants utilisent de tels logiciels.)

4 Les techniques de protection

Les techniques de protection abordées dans le présent rapport sont :

- l'incorporation de données, sous la forme :

  de *filigrane*, *visible* ou *invisible*, qui se veut une marque d'identification infalsifiable et indélébile de la *source* d'une image,

  d'*empreinte d'identification*, une marque d'identification infalsifiable et indélébile qui identifie le *destinataire* de la copie d'une image,

- le *chiffrage*, qui vise à protéger le contenu d'un ensemble de données contre toute utilisation non autorisée,

- la *technique des conteneurs*, qui permet la superdiffusion protégée de données par tout usager, qu'il possède ou non une licence.

Toutes ces techniques sont utilisées à des degrés divers par les systèmes de gestion des droits d'auteur. Nous croyons que le *chiffrage* et les *conteneurs* constitueront vraisemblablement l'assise de tout système complet de gestion des droits d'auteur [Jurenka, 1997], mais le filigrane et les techniques d'incorporation de données se prêtent plus aisément à la commercialisation de produits offrant des protections précises, et sont donc plus susceptibles d'être visibles sur le marché des moyens techniques de protection des images.

4.1 Types de filigrane

Sur une feuille de papier, le filigrane se présente comme un dessin gravé ou pressé dans le papier et qui peut se voir par transparence. Dans un document sur support électronique, le filigrane peut être visible ou invisible. Un filigrane visible est habituellement une image estompée superposée sur l'image principale qui, si elle est réussie, donnera l'impression d'être « en arrière-plan », comme si l'image à l'écran était une représentation d'un original imprimée sur papier filigrané. Souvent, un filigrane invisible n'est pas une image mais une série de bits cachée dans une image ou dans un fichier sonore et qui est récupérée du fichier à l'aide d'une application de décodage.

Une fonction d'un filigrane numérique visible est de rendre apparent à un usager le fait qu'un document est la *propriété* de quelqu'un et qui en est le propriétaire. Il est plus facile et plus discret d'inclure un avis de droit d'auteur. Par contre, comme l'avis de droit d'auteur ne figure que dans une partie du document, à part du contenu, il ne paraîtra pas dans un extrait tel qu'une image recadrée, alors que les filigranes visibles sont conçus pour être visibles dans une grande partie de l'image, tout comme les filigranes sur papier.

Un filigrane visible devrait être lui-même un dessin assez complexe pour être difficile à contrefaire. Malheureusement, il est facile de se procurer la technologie nécessaire pour incorporer des

filigranes dans des images numériques, et comme on peut écrire des programmes pour récupérer un filigrane d'une image numérisée, toute personne compétente munie d'un ordinateur de bureau peut réussir une contrefaçon numérique. Pour éviter que cela ne se produise, on peut créer une « licence » en direct, dont les conditions doivent être acceptées par l'usager pour que celui-ci ait accès à une image et qui lui interdit *toute* modification de l'image. Mais cette façon de procéder, pourtant largement répandue, n'est pas forcément efficace. Prises à la lettre, ces ententes rendent inutilisables, même à des fins légitimes, les images protégées par un contrat de licence. Par exemple, réduire une carte en couleurs à une gamme de gris, afin de l'imprimer en noir et blanc, constitue bel et bien une modification.

Grâce à une technique spéciale, qu'utilise d'ailleurs le *Picture Information Network* (PNI) [Walter, 1995], il est possible de créer des filigranes numériques qui ne sont visibles que lorsque l'image est imprimée et qui ne s'affichent pas à l'écran. Cette méthode découle de techniques mises au point pour empêcher la contrefaçon de documents financiers à l'aide de photocopieurs ou d'imprimantes à laser et est tributaire de caractéristiques particulières de ces appareils modernes.

Les filigranes invisibles ont également pour but de noter la *source* légale d'un document (par exemple le détenteur du droit d'auteur), mais d'une manière indétectable par l'usager. Cette dernière caractéristique est essentielle dans le cas de fichiers audio et fortement souhaitable dans le cas d'images. Le filigrane doit aussi être *robuste* davantage que ne l'est l'avis habituel de droit d'auteur : le filigrane doit résister aux tentatives de suppression ou d'altération et doit survivre à des transformations telles que le détourage, l'altération des couleurs d'une image ou la suppression des moments de silence dans un fichier audio, de telle sorte que le filigrane reste présent dans une éventuelle copie comme preuve de propriété.

Même si la robustesse d'un filigrane est traitée comme capitale dans les comptes rendus de recherche, il est à noter que dans certains cas elle peut ne pas être très importante pour la mise en application des droits. Si la propriété de l'original d'une image ne fait pas de doute et si l'on dispose de l'original comme preuve, comme dans le cas des images qui appartiennent à une bibliothèque ou à un musée, la diffusion d'une image numérique dont on a supprimé le filigrane peut constituer *en soi* une preuve juridique d'une violation du droit d'auteur. Les articles 11 et 12 du traité de 1996 de l'OMPI (Organisation mondiale de la propriété intellectuelle) sur le droit d'auteur [OMPI, 1996] constituent en droit international un cadre juridique, servant de fondement à des lois nationales (telles que le *Digital Millennium Act* des États-Unis), qui interdit le retrait de dispositifs de protection des droits tels que le chiffrage et l'information sur ces droits, ce qui inclut les éléments d'identification contenus dans les filigranes.

4.1.1 Filigranes visibles

Il y a sans doute lieu de faire remarquer ici que l'incorporation de filigranes visibles dans des images n'est pas une opération difficile du point de vue algorithmique. De fait, tout programmeur en langage C qui possède une expérience des formats et de la manipulation des images est en mesure de concevoir des filigranes raisonnables. Les musées qui désirent incorporer un filigrane visible dans les images d'une collection ne sont donc pas obligés de recourir à un logiciel spécifique ni aux services d'un tiers. Ils peuvent, si les besoins le justifient, produire leurs propres filigranes.

La *superposition* d'un filigrane peut affecter la beauté d'une image. Le filigrane peut être perçu comme une « violence » faite par exemple à la figure d'une personne représentée. Cela peut choquer un certain public ou être considéré par l'artiste comme une violation de ses droits moraux. Autre exemple susceptible de choquer : l'altération d'une image tenue pour sacrée par un groupe religieux.

Pour éviter de tels effets négatifs, les usagers peuvent devoir utiliser un logiciel de visionnement dont une option permet la suppression du filigrane à l'aide d'une touche particulière lorsqu'un fichier d'image est sélectionné. Cela semble une caractéristique souhaitable puisqu'elle permet de préserver pour l'usager la valeur esthétique, humaniste ou évocatrice d'une image. Par contre, pour qu'une option de ce genre soit effective, il faut veiller à former les usagers quant à son existence et à ses implications.

Le choix d'un motif de filigrane pour des images dont la qualité visuelle et graphique varie grandement doit tenir compte de nombreux facteurs pour donner l'effet recherché. Il faut noter qu'un filigrane visible est facile à supprimer à l'aide de logiciels graphiques du domaine public. Cette opération peut s'effectuer en quelques minutes avec un micro-ordinateur et un logiciel de traitement d'images disponible dans le commerce. Comme on le fait remarquer dans la foire aux questions de Digimarc [traduit de Digimarc, s. d.] : « Comme un filigrane visible est visible et localisé, le supprimer est un jeu d'enfant. »

Les problèmes qui se posent avec les filigranes visibles les rendent moins attrayants comme moyen de protection. IBM, qui utilisait des filigranes visibles au début de son projet pour la Bibliothèque du Vatican, a décidé que ce moyen était « inapproprié pour des œuvres d'art. Lorsque le filigrane est en évidence, il nuit au contact du visiteur avec l'œuvre d'art. Lorsque le filigrane est peu apparent, le visiteur se demande ce qui appartient à l'œuvre et ce qui fait partie du filigrane. » [traduit de Mintzer, 2000] C'est pourquoi le projet d'IBM pour le Musée de l'Hermitage ne fait appel qu'à des filigranes invisibles pour la protection des images en ligne à grande résolution.

4.1.2 Filigranes invisibles

Les filigranes invisibles appartiennent à la discipline émergente de la « dissimulation de données » ou *stéganographie*. Les objets multimédias, en particulier les extraits sonores et les images, comportent inévitablement des bits que l'on peut modifier imperceptiblement. On peut exploiter cette caractéristique de bien des manières pour coder à l'intérieur de l'objet une information externe, sous le seuil de détection auditive ou visuelle. (En général, on ne peut pas incorporer un filigrane invisible dans des images simples produites par ordinateur ou dans un texte en ASCII.)

Dans le cas des filigranes visibles, l'information ajoutée à une image est volontairement visible, afin que la source de l'image puisse être reconnue d'emblée. Dans le cas des filigranes invisibles, il est important que l'information ajoutée *ne puisse pas* être détectée lors d'un examen auditif ou visuel, afin qu'elle ne puisse pas être supprimée, et qu'elle ne dégrade pas l'image, mis à part peut-être une légère baisse de qualité. Il faut toutefois que l'on puisse détecter et récupérer le filigrane à l'aide d'un logiciel particulier.

La différence entre la technique du filigrane invisible et le chiffrage est que ce dernier rend l'objet inutilisable, alors que la présence du filigrane ne devrait pas interférer avec l'utilisation de l'objet. Le filigrane est typiquement créé et incorporé à l'aide d'une clé secrète élaborée par le créateur de l'objet numérique. Il faut connaître cette clé pour pouvoir détecter et décoder le filigrane dans une image. C'est donc généralement le créateur de l'objet, et non l'utilisateur, qui effectue la vérification. Dans certains cas, l'original de l'image doit également être disponible pour permettre la détection du filigrane.

Les filigranes qui sont détectables sans accès au contenu original permettent d'utiliser un robot [Cheong, 1996] qui parcourt le Web d'un site à un autre à la recherche de fichiers qui contiennent un filigrane précis. Un tel robot peut constituer un moyen très peu coûteux de recueillir des données sur l'origine et le degré des violations du droit d'auteur partout dans le monde.

Les images numériques sont très souvent transformées par compression avant diffusion, redimensionnement ou détourage. Les techniques de filigrane doivent donc être suffisamment robustes pour résister, à tout le moins, à la compression et aux transformations géométriques de l'image.

Il est également souhaitable que le filigrane soit réparti dans toute l'image afin que son existence puisse être détectée dans une partie de l'original. Idéalement, le filigrane devrait résister à l'impression, de sorte que si l'image imprimée est numérisée à nouveau, le filigrane puisse être détecté [Cox, I., 1996].

Une caractéristique importante du filigrane, par comparaison avec d'autres techniques de protection telles que le chiffrage, est qu'il permet de protéger des documents audio et vidéo même lorsqu'ils sont convertis du mode numérique au mode analogique. S'il est bien fait, le filigrane peut même être récupéré dans une bande audio ou vidéo enregistrée à partir de la sortie du document numérique sur les haut-parleurs ou à l'écran de l'ordinateur, ou encore en interceptant le signal électronique de la carte son ou de la sortie vidéo de l'ordinateur.

L'utilisation principale du filigrane invisible, tout comme du filigrane visible, est de donner au propriétaire du contenu protégé par le droit d'auteur le moyen de prouver qu'il est propriétaire des données stockées dans ce contenu et de prouver le cas échéant qu'il y a eu violation du droit d'auteur. Au contraire d'un filigrane visible ou d'un avis de droit d'auteur, un filigrane invisible est typiquement différent d'une image à l'autre. Il peut contenir un identificateur de production, un horodatage, des données sur le droit d'auteur et sur les utilisations autorisées, etc., dans la limite de la taille possible du filigrane (en général jusqu'à quelques milliers de bits, soit quelques centaines de caractères).

Comme pour la cryptographie, les techniques de filigrane invisible, et de stéganographie en général, reposent sur l'application de concepts mathématiques évolués mais leur mise en œuvre n'exige pas de matériel ou de logiciel particulier. Ce domaine convient donc très bien à la recherche universitaire et, grâce à l'émergence d'un marché pour des produits de filigrane, de nombreux algorithmes de filigrane ont fait leur apparition dans les publications de recherche. Les

sites gérés par Hartung et Peticolas [Hartung, 1997 et Petitcolas, 2000] contiennent des liens utiles vers des travaux actuels dans ce domaine. [Voyatzis, 1999] résume bien les rôles et les exigences de la réalisation de filigranes.

La recherche dans le domaine des filigranes a été stimulée par la vulnérabilité de certains des premiers algorithmes. Le repérage d'attaques possibles et les propositions pour les contrer ont donné lieu à de nombreuses publications dans ce domaine. Un certain scepticisme sur la protection réelle que procurent les filigranes vient de ce que les algorithmes des produits disponibles dans le commerce sont secrets, même s'ils sont probablement fondés sur de la recherche publiée. Dans le domaine connexe de la cryptographie, on sait depuis longtemps que les algorithmes secrets ne sont pas aussi dignes de confiance que ceux qui sont publiés. En effet on peut analyser ces derniers, les soumettre à des attaques expérimentales et mettre en œuvre des améliorations en profitant de l'expérience acquise par une communauté d'experts sur ces algorithmes. (Voir une discussion vivante et non technique dans [Schneier, 2000].) Les algorithmes secrets peuvent être percés — le secret peut être volé ou découvert — mais il n'est pas possible de les améliorer en les analysant et en les défiant. C'est ce qui a motivé la réalisation du banc d'essai *StirMark* [Kutter, 1999 et Petitcolas, 1999] pour les produits de filigrane, qui fournit un système de notation indépendant faisant appel à des techniques ouvertes faciles à reproduire, au lieu de se fier à des affirmations de fournisseurs impossibles à vérifier.

Comme en cryptographie, on risque fort d'assister à un scénario de « course aux armements » : les fournisseurs tentent d'améliorer petit à petit leurs produits en relevant chaque nouveau défi, alors que les experts continuent d'en rechercher et d'en publier les points faibles. À court terme, il est probable qu'il y aura des victoires et des défaites dans les deux camps, avec pour résultat que la technologie continuera d'évoluer et de s'améliorer.

4.1.3 Filigranes fondés sur la méthode DCT

Les algorithmes de filigrane opèrent souvent dans le *domaine spatial* des images : ils repèrent dans l'image des endroits appropriés qui sont ensuite altérés par l'ajout d'information du filigrane. L'inconvénient de ces méthodes est que le filigrane résiste mal aux transformations de l'image. Une autre méthode fait intervenir une représen-tation de l'image dans un domaine bidimensionnel de *fréquences* (analogue à l'analyse unidimensionnelle d'un signal acoustique en termes de fréquences plutôt que d'ampli-tudes) à l'aide de la méthode DCT (*Discrete Cosine Transformation* — transformée discrète en cosinus). (Cette transformation est à la base de l'algorithme de compression JPEG, très employé pour les images.) L'ajout du filigrane dans l'image se fait par mani-pulation des coefficients de fréquence dans la DCT, puis la représentation résultante de l'image dans le domaine des fréquences est reconvertie dans le domaine spatial à l'aide de la transformée inverse de la DCT. Une combinaison de la méthode DCT et de la méthode spatiale consiste à déterminer des zones précises de l'image où l'on applique la méthode DCT. Cette détermination peut être pseudo-aléatoire, comme dans l'algorithme utilisé par *SysCoP*, ou reposer sur des critères tels que la sensibilité au bruit.

Cappellini et son équipe de l'Université de Florence [Barni, 1998] ont mis au point un algorithme évolué fondé sur la méthode DCT. Cet algorithme produit des filigranes détectables sans la

présence de l'image originale et qui résistent bien à une vaste gamme d'attaques, dont :

- des transformations géométriques (redimensionnement, détourage, etc.),
- la compression JPEG,
- les filtres passe-bas,
- les filtres médians,
- l'inversion de lignes,
- l'ajout de filigranes supplémentaires.

4.1.4 Suivi de l'utilisation

Au lieu ou en plus d'utiliser le filigrane numérique pour décourager la copie ou l'altération de documents, on peut incorporer dans le document lui-même de l'information sur son utilisation. C'est ce que l'on appelle une *empreinte numérique* — la création d'un enregistrement invisible de données sur l'usager, établi à partir de l'information recueillie lorsque la diffusion de l'image à l'usager a été autorisée. Si le document apparaît ensuite dans un contexte donnant à penser qu'il a été illégalement copié ou transféré, on peut retrouver l'identification de l'usager initialement responsable de la violation des droits ou des conditions de la licence. Comme dans le cas des signatures numériques, les empreintes numériques sont plus ou moins faciles à réaliser selon le contenu du document. Les documents volumineux et qui ont un certain niveau de bruit comme les photographies et les extraits sonores favorisent cette opération.

Les techniques stéganographiques employées pour créer des filigranes invisibles permettent également de produire des empreintes numériques. On croit que la présence d'un historique des transactions caché dans la copie de l'usager et difficile à modifier ou à supprimer dissuadera les gens honnêtes « de faire des choses malhonnêtes. Les usagers sont moins susceptibles de quitter le droit chemin s'ils savent qu'ils laissent leur empreinte. » [traduit de Cognicity, 2000].

4.2 Le chiffrage

Le chiffrage numérique est la transformation mathématique d'un ensemble de données pour qu'il ne puisse être « lu » ou utilisé que par quelqu'un qui possède une information secrète donnée, la clé de déchiffrage, qui sert à inverser la transformation mathématique et à restituer les données originales.

Le chiffrage sert à diverses fins dans le contexte de la circulation à l'intérieur d'un réseau d'information protégée par le droit d'auteur ou par une licence :

- Il empêche le « vol » *pendant le transit*. À l'heure actuelle, la plupart des réseaux, et plus particulièrement Internet, ne sont pas sûrs. Les données passent par de nombreux serveurs entre l'expéditeur et le destinataire. Ces ordinateurs peuvent, en principe, détecter et recueillir l'information qui circule chez eux. (C'est pour cette raison que les mots de passe, les numéros de carte de crédit et tout identificateur du même genre ne devraient jamais être transmis par Internet sans avoir d'abord été chiffrés ou avoir fait l'objet de mesures de sécurité particulières.)

- Le chiffrage peut servir à demander au destinataire d'exécuter une opération supplémentaire, comme d'obtenir un « mot de passe » ou une clé de déchiffrage, afin de déchiffrer et de visionner l'information. C'est la méthode qu'adoptent souvent les fournisseurs de disques optiques compacts contenant des collections de polices de caractères ou des jeux. Une méthode semblable exige que l'usager tape un mot de passe de son choix à des fins d'authentification. Ce mot de passe déclenche automatiquement la transmission de la clé de déchiffrage à une application présente dans l'ordinateur de l'usager. (C'est la méthode employée pour la transmission sécuritaire de données de l'utilisateur vers un site Internet.)

- Il se peut que l'usager doive se servir d'un logiciel spécial qui, tout en permettant de déchiffrer et d'afficher le contenu, ne lui permet pas de se servir des fonctions normales du système d'exploitation, comme la copie ou les fonctions *copier-coller*, ce qui a pour effet de protéger le contenu — dans une certaine mesure — contre les modifications et la rediffusion.

Les techniques de chiffrage classiques font appel à la même clé pour le chiffrage et le déchiffrage. Ainsi, l'expéditeur et le destinataire doivent *partager* un secret. Ceci pose de grandes difficultés pour la diffusion d'information dans un réseau de télécommunications où l'expéditeur et le destinataire ne peuvent vraisemblablement pas se rencontrer face à face pour se transmettre la clé en toute sécurité, et où l'expéditeur n'a pas de garantie que le destinataire va garder le secret qui lui a été confié.

Grâce à l'innovation technique appelée *cryptographie à clé publique* [Fahn, 1993], le chiffrage est maintenant devenu un outil pratique pour la protection de l'information numérisée. Suivant cette technique, une personne crée une paire de clés sous forme de longues suites de lettres ou de chiffres (souvent à l'aide d'un logiciel) — une clé publique, qui est publiée ou mise à la disposition de quiconque désire envoyer un message chiffré à la personne qui a créé la clé publique, et une clé privée qui reste secrète de telle sorte que seule la personne qui l'a créée puisse s'en servir pour déchiffrer un message. Il existe un lien mathématique entre les clés de la paire afin que les messages chiffrés à l'aide de la clé publique puissent être déchiffrés à l'aide de la clé privée. Voici un exemple simplifié de la manière dont cela fonctionne, inspiré de l'histoire d'un couple bien connu dans le monde des messages secrets, Roméo et Juliette :

> Supposons que Juliette veut envoyer à Roméo un message secret que seul Roméo pourra lire. Juliette recherche la *clé publique* de Roméo ou la lui demande (il s'agit d'une longue suite de caractères apparemment aléatoires). Cette clé n'étant pas secrète, Roméo la lui envoie par courrier électronique ou Juliette vient la chercher dans ses pages Web. Juliette insère la clé dans son logiciel de chiffrage et tape son message. Le résultat : un fichier incompréhensible de caractères apparemment aléatoires, qu'elle envoie à Roméo. Roméo utilise son logiciel de chiffrage dans lequel il a inséré ses clés privées pour lire le message.

Ce qu'il faut retenir ici, c'est que Roméo et Juliette n'ont pas été obligés de partager un secret pour que le message soit transmis en toute sécurité.

En pratique, seuls de très courts messages sont chiffrés par cryptographie à clé publique, en raison de la complexité des calculs qu'exige la méthode. La pratique courante veut plutôt qu'on utilise une clé publique pour chiffrer *une autre clé* qui sera utilisée dans le cadre d'une technique à clé

secrète comme la très populaire DES (*Data Encryption Standard* ou norme de chiffrage des données). L'expéditeur chiffre le message réel en se servant de cette clé secrète, et le destinataire déchiffre le message au moyen de la clé qu'il a tout d'abord déchiffrée au moyen de sa clé privée.

Les logiciels de chiffrage DES sont largement accessibles et considérablement plus rapides que les algorithmes de clés publiques. Pour chiffrer une image, il suffit de diviser cette image en blocs de, mettons, 64 octets. Chaque bloc est chiffré et déchiffré au moyen d'une clé de 64 octets qui brouille et décode le contenu de chaque bloc.

Voici un exemple simplifié de la façon dont la transmission d'une image pourrait s'effectuer à partir d'une base d'images (appelée Juliette) à destination de l'utilisateur Roméo :

> Roméo choisit une image à partir d'une liste présentée par un navigateur. Le navigateur transmet la demande au serveur de Juliette et inclut une clé publique qui ne sera utilisée que pour cette opération. (La clé publique n'est pas secrète et peut donc être transmise sur les voies non protégées d'Internet). Le serveur Juliette chiffre une clé DES (qui ne sera utilisée que pour cette opération) avec la clé publique de Roméo et renvoie la clé chiffrée à Roméo. Cette technique est très sûre puisque si la clé venait à être interceptée pendant la transmission, elle ne pourrait pas servir sans la clé privée du navigateur de Roméo. Juliette chiffre alors l'image choisie avec la clé DES et transmet le bloc chiffré au navigateur de Roméo, qui utilise la clé DES qu'il a reçue pour déchiffrer et faire afficher l'image.

Il y a lieu de noter que dans ce scénario, Roméo, l'utilisateur ultime, ne participe d'aucune façon aux opérations cryptographiques effectuées par son logiciel de navigation.

4.2.1 Les signatures d'authentification

La cryptographie à clé publique peut servir à *authentifier* la source d'un document (image, etc.). En effet, elle permet, par une vérification mathématique, de s'assurer que l'entité qui dit être la source a accès à la clé privée qui correspond à la clé publique de la source. La procédure (quelque peu simplifiée) est la suivante :

> Supposons que Roméo veut vérifier si le message chiffré qu'il a reçu provient bien de Juliette. Comme Juliette a utilisé la clé publique de Roméo pour le chiffrage, Roméo utilise sa clé privée pour déchiffrer le message, qui contient une « signature » que Juliette avait chiffrée avec sa clé privée. La « signature » n'est pas propre à Juliette, comme le serait sa signature manuscrite, mais est plutôt une quantité tributaire du *message*. C'est un nombre de longueur fixe qui a été calculé à partir du message et qui a comme propriété d'empêcher quiconque de déterminer quels messages ont pu produire la valeur de la signature. Mais Roméo a accès au message lui-même puisqu'il vient de le déchiffrer. Il peut alors appliquer la procédure de signature (s'il ne sait laquelle utiliser, Juliette pourrait le lui indiquer dans le message) au message et vérifier s'il obtient bien la « signature ». Dans l'affirmative, le message ne peut provenir que de quelqu'un ayant accès à la clé privée de Juliette, donc en principe de Juliette.

Bien que l'authentification soit un aspect important de la cryptographie à clé publique, elle n'est pas aussi utile dans le domaine de la diffusion d'images numérisées. Dans ce cas, on emploie une autre méthode, aussi appelée *signature numérique*. Il en est question à la section 4.3.

4.2.2 Logiciel ou matériel

Pour protéger le contenu des fichiers, les diffuseurs d'images utilisent en général des formats de fichier et des algorithmes de chiffrage qui leur sont propres et qui exigent l'acquisition d'un logiciel spécifique de visualisation pour pouvoir décoder les images. Le fournisseur de contenu doit donc inclure dans ce logiciel un secret (la méthode ou la clé de déchiffrage) et espérer que l'usager ne tentera pas de percer ce secret, par exemple en analysant le code du logiciel. De plus, le fournisseur doit supposer que l'usager sera suffisamment intéressé par le contenu pour télécharger le logiciel de visualisation ou accepter un téléchargement automatique de ce logiciel. Mais exiger des usagers qu'ils acquièrent et installent un logiciel ou un plugiciel particulier pour chaque algorithme de chiffrage disponible dans le commerce ne semble pas une proposition viable, à moins qu'une technologie unique n'en vienne à dominer le marché ou que des normes soient imposées.

Une telle norme pourrait par exemple ressembler au schéma de protection du groupe IBM/4C [Lehmann-Haupt, 2000], qui repose sur une approche très différente — le contenu est chiffré d'une manière telle qu'il ne peut être déchiffré que par des *appareils de stockage et de lecture compatibles*. L'application initiale vise la création de lecteurs MP3 qui ne joueront que des copies autorisées, mais le concept peut être étendu à des disques rigides et donc au contrôle physique de la copie d'images dans le micro-ordinateur de l'usager. IBM et d'autres fabricants ont déjà des normes de ce genre pour des lecteurs de disques [Orlowski, 2001]. [Schneier, 2001] donne certains détails sur les questions liées à la protection intégrée dans des lecteurs de disques rigides.

On ne sait pas encore si les fabricants d'appareils, de concert avec les fournisseurs de contenu, arriveront à mettre en œuvre le chiffrage physique dans l'ensemble du marché de la micro-informatique. Mais s'ils y parviennent, il est probable que les sanctions contre la fraude et le contournement de ces dispositifs rendront les attaques plus coûteuses et que les formes actuelles de violation par copie pour des raisons de commodité ou de partage diminueront considérablement, sans toutefois disparaître complètement, comme ce fut le cas dans d'autres domaines tels celui du décodage des signaux transmis par câble.

4.2.3 Contournement du chiffrage par des moyens logiciels

Si un diffuseur d'images chiffrées exige un logiciel ou plugiciel spécial de déchiffrage et de visualisation, il est souhaitable que le fichier se présente dans un format standard (p. ex., JPEG) pour être facilement télédéchargé à l'aide d'un logiciel de navigation tel que *Netscape* ou *Internet Explorer*. Le fichier est présent dans le disque rigide de l'usager (par exemple, dans l'antémémoire du navigateur). Cependant, il paraît vide pour un logiciel de visualisation JPEG ordinaire en raison du chiffrage. L'application ou le plugiciel qui permet à l'usager de voir l'image n'autorise habituellement pas la copie ou l'impression, et comme ce n'est pas le navigateur qui commande l'affichage, ses commandes de copie et d'impression sont inopérantes pour la fenêtre de l'image. Cela n'empêche toutefois pas l'usager de copier et de manipuler l'image. Il suffit de quelques opérations pour saisir la totalité de l'écran, y compris l'affichage produit par le logiciel de visualisation, et l'enregistrer dans un fichier standard non chiffré.

Cela peut se faire parce que l'image est nécessairement présente en mémoire sous une forme non chiffrée pour pouvoir être affichée, sans que la commande du système d'exploitation qui permet de saisir un écran et de l'enregistrer dans un fichier n'ait été mise hors service. Même si l'application de visualisation met temporairement hors service la saisie d'écran (ce qui est le cas de *Vyoufirst*), cela n'empêche pas nécessairement de copier le contenu déchiffré, car il est bien possible d'écrire un programme capable de faire l'équivalent d'une saisie d'écran, c'est-à-dire trouver en mémoire les données qui constituent l'image et les copier dans un fichier.

Si l'usager se sert de mémoire virtuelle (ou paginée) pour étendre la capacité de mémoire de son ordinateur, le contenu déchiffré créé en mémoire à partir d'un document chiffré peut à un moment donné être transféré par le système d'exploitation dans la partie d'un disque qui sert d'extension de la mémoire (l'espace de pagination), où ce contenu peut facilement être saisi à l'aide d'outils standard de gestion de disques même s'il n'a jamais été explicitement enregistré sous forme d'un fichier. Certains logiciels de chiffrage populaires sont vulnérables à des attaques de ce genre [Rowan, 1997].

4.2.4 Lien entre compression et chiffrage

La compression réduit les répétitions ou les motifs dans un fichier, ce qui favorise le chiffrage en diminuant les redondances. De plus, la compression réduit la taille du fichier de données, ce qui diminue d'autant le travail requis de la part de l'ordinateur pour exécuter l'algorithme de chiffrage. Par conséquent, un algorithme rapide de compression améliore la sécurité et le rendement d'un algorithme de chiffrage.

Si l'on utilise un algorithme de compression comme JPEG et un algorithme de chiffrage comme DES, il ne faut jamais chiffrer le fichier avant de le comprimer. Un bon algorithme de chiffrage produit un résultat qui, sur le plan statistique, ne se distingue pas de nombres aléatoires, et les algorithmes de compression ne peuvent pas réduire la taille d'un fichier de nombres aléatoires (en fait l'algorithme JPEG pourrait faire *augmenter* la taille d'un tel fichier.)

Cependant, l'application du chiffrage de type DES à des images comprimées présente des inconvénients, comme le soulignent Macq et Quisquater [Macq, 1994] :

- L'auteur peut vouloir protéger ses images indépendamment du processus de transmission, donc indépendamment de l'algorithme de compression utilisé, et avant la transmission.

- Les techniques de compression sont très sensibles aux erreurs de transmission, qui peuvent être évitées par l'ajout de données supplémentaires de format et de synchronisation. Ces données supplémentaires ne doivent pas être chiffrées, car dela diminuerait l'efficacité du chiffrage. Par contre, si on les omet, on augmente les risques d'erreur de transmission.

- Dans de nombreuses applications, le chiffrage devrait être partiellement transparent : par exemple, des miniatures ou des extraits stockés dans le fichier d'image ne devraient pas être chiffrés ou ne l'être que partiellement. (Comparer avec le système TIE décrit plus loin.)

C'est pourquoi Macq et Quisquater [Macq, 1994] ont proposé une technique de chiffrage des images qui prévoit de chiffrer le fichier avant de le comprimer. Ils mettent de l'avant un système à résolution multiple qui produit une image compressible associée à un degré de transparence donné.

Selon cette technique, seules les portions de l'image correspondant à un niveau de détail donné (c.-à-d. à grande résolution) sont chiffrées, de sorte que l'on obtient une image chiffrée qui possède les mêmes propriétés statistiques qu'une image non chiffrée et qui est donc compressible.

4.3 Techniques d'incorporation de données

Dans cette section, nous examinons brièvement trois produits de protection disponibles dans le commerce. Ces produits font appel à la technique du filigrane numérique et, plus généralement, à des données cachées incorporées dans le contenu numérique. (Les coordonnées des fournisseurs des produits mentionnés figurent dans la section *Fournisseurs et organismes* de ce rapport.)

4.3.1 Cognicity

Cognicity offre un outil de filigrane, *Audio Key*[MC], qui incorpore des données dans une image ou un signal audio ou vidéo sans affecter la qualité du contenu. Ce filigrane est très robuste et conserve son intégrité même lorsque l'original est modifié, comprimé ou converti d'un format à un autre. Cognicity prétend que le filigrane persiste même si le contenu numérique est converti sous forme analogique.

Il existe également une version professionnelle de *AudioKey*, appelée *AudioKey Pro*, qui permet d'incorporer des restrictions d'accès au contenu numérique pour des utilisateurs précis pendant une période de temps donnée.

AudioKey peut être couplé à un autre produit de Cognicity, *Audio Key MP3*[MC], qui incorpore directement dans le contenu numérique un registre des transactions antérieures portant sur ce contenu. Ce registre commence par la transaction initiale et peut contenir de l'information sur le propriétaire du contenu, l'identification du contenu, des données sur le fournisseur et sur les transactions. Les données de ce registre permettent au propriétaire de vérifier la propriété réelle du contenu et tout « partage » ou piratage de ce contenu au cours de sa vie utile.

4.3.2 Digimarc

La société Digimarc a mis au point une technique largement publicisée pour incorporer des signatures électroniques ou d'autres types d'information directement dans des photographies, des documents visuels et sonores, ainsi que d'autres documents de création fondés sur des données du « monde réel ». Cette technique ne s'applique pas aux images créées par ordinateur ni aux textes en format ASCII.

Pour créer un filigrane Digimarc (qui portait autrefois le nom de *signature*), il faut combiner, avec l'information à incorporer aux données, un code, aléatoire en apparence, qui soit propre à l'auteur. Le filigrane peut être ajouté à l'image à l'aide d'un plugiciel utilisé en conjonction avec un logiciel de traitement d'images tel que *Adobe Photoshop*. Il n'est pas possible d'ajouter un filigrane Digimarc à une image numérique qui contient déjà un filigrane.

Le filigrane est ajouté à l'image numérisée (ou à toute autre œuvre de création) à un niveau de signal inférieur au « bruit » ou à l'allure aléatoire inhérente aux données. L'usager ne peut donc pas voir le filigrane, qui est par contre facile à récupérer à l'aide du code unique du créateur et qui ne peut pas être décelé ou supprimé sans accès au code en question. Le filigrane Digimarc est réparti dans toute l'image, ce qui permet de détecter des modifications subséquentes, comme dans les cartes d'identité avec photo.

Cette technique est présentée comme un moyen d'assurer aux créateurs qu'ils pourront prouver les cas de contrefaçon plutôt que les empêcher. Le robot *MarcSpider*[MC] permet de chercher dans le Web des images contenant le filigrane de Digimarc. Digimarc offre à ses clients un abonnement de suivi du contenu numérique à l'aide de *MarcSpider*. L'abonné reçoit des rapports Web sur l'utilisation de son contenu pendant la période d'abonnement.

Ce service de suivi utilise les principaux moteurs de recherche du Web pour trouver les documents filigranés en cours d'utilisation. Par contre, ce service ne peut détecter des utilisations des images que dans les sites déjà indexés. La page Web de Digimarc contient l'avis de non-responsabilité suivant à propos de *MarcSpider* :

> « Cela signifie que *MarcSpider* ne trouvera probablement pas toutes vos images filigranées, en particulier si elles font partie de sites qui ne sont pas indexés de manière intensive dans les principaux répertoires et moteurs de recherche. » [traduit de Digimarc]

Digimarc soutient que sa technique sert à de nombreux usages. En plus de la preuve de propriété, les filigranes peuvent contenir d'autres renseignements comme :

- les droits de licence,
- les règles et restrictions d'utilisation,
- les données sur la création, dont les données sur la caméra,
- la filière de diffusion,
- de l'information sur les ressources concernant les systèmes de gestion des droits d'auteur,
- l'identification du contenu, par exemple des légendes ou des avertissements à propos de contenu réservé aux adultes.

Digimarc soutient que, contrairement à d'autres techniques de protection du droit d'auteur, les signatures de Digimarc peuvent identifier le propriétaire et donner d'autres renseignements sur l'image ou la propriété intellectuelle sans interdire complètement l'accès à l'image (comme c'est le cas avec le chiffrage), ni séparer ces renseignements de l'image elle-même (comme c'est le cas des en-têtes de fichier), ni altérer l'image (comme le filigrane, les miniatures ou la réduction de la résolution).

4.3.3 MediaSec

SysCoP (*System for Copyright Protection* ou système de protection du droit d'auteur) a été mis au point à l'institut d'infographie Fraunhofer (de Darmstadt, en Allemagne) par J. Zhao, et est maintenant commercialisé par la société MediaSec Technologies. Comme c'est le cas pour les techniques de Cognicity et de Digimarc, l'étiquette incorporée est réputée invisible, indélébile et résistante aux altérations dues à la compression ou au changement de format de fichier.

MediaSec donne la liste suivante des renseignements habituellement inclus :

- l'avis de droit d'auteur,
- l'origine et le propriétaire,
- la destination ou la transaction,
- les permissions d'utilisation,
- les caractéristiques du document.

SysCoP permet d'inclure plusieurs types de filigrane :

- Un filigrane hiérarchique incorpore plusieurs jeux de renseignements dans un document multimédia, de sorte que chaque jeu peut être extrait indépendamment des autres pour permettre le suivi d'une chaîne de transactions sur le droit d'auteur.
- Un filigrane localisé permet d'inclure une étiquette à l'intérieur ou à l'extérieur d'une partie précise des données multimédias.
- Un filigrane public permet d'inclure des renseignements qui peuvent être lus sans recours à une clé secrète.

Selon les auteurs de *SysCoP*, la compression avec perte d'information (comme dans le format JPEG), les conversions de format, le filtrage passe-bas, la réduction des couleurs, l'impression, la lecture optique, la rotation, le changement d'échelle ou le recadrage n'affectent pas le filigrane.

Comme le montre le tableau ci-dessous, SysCoP fonctionne sur des images fixes, des images animées et des textes en format Postscript :

Type de document	Formats reconnus
Image	PPM, PGM, GIF, TIFF
Vidéo	MPEG-1, MPEG-2
Images de pages mises en forme	Postscript

Les méthodes sont quelque peu différentes selon le support, mais toutes comportent deux étapes fondamentales. La première consiste à générer une suite pseudo-aléatoire de positions pour sélectionner des blocs où les données seront incorporées. Cette étape fait appel à des données extraites de l'image et à une clé secrète choisie par le fournisseur de contenu comme valeur de départ de la suite pseudo-aléatoire. La seconde étape consiste simplement à incorporer ou à

récupérer le code dans ou à partir des blocs précisés dans la suite de positions au moyen de diverses méthodes d'étiquetage. Il faut noter que contrairement à la plupart des techniques d'incorporation de données, qui ne fonctionnent qu'avec des images « naturelles » (ou des fichiers audio), les méthodes de *SysCoP* s'appliquent aussi à des textes.

Le projet TIE de l'institut Fraunhofer de Darmstadt a donné lieu à la mise au point d'un serveur d'images avec *portions chiffrées*, qui permet d'afficher une partie de l'image sans logiciel particulier autre que le navigateur de l'usager. MediaSec offre maintenant cette technique de chiffrage sélectif dans son produit *MediaCrypt*[MC], dans lequel les données originales des zones brouillées sont annexées au fichier d'image et transmises sous forme chiffrée.

4.4 Techniques de conteneurs étanches

Les *conteneurs* sont des modules logiciels qui contiennent plusieurs ensembles de données différentes. Lorsque l'utilisateur y a accès, le conteneur lance les processus appropriés, comme le chiffrage, la visualisation, etc. Le conteneur n'est pas un objet inerte comme un fichier de données qui peut être ouvert et manipulé au moyen de diverses applications. Il comprend des instructions aussi bien que des données et ne peut être lu ou modifié que dans des conditions bien précises.

Les techniques des conteneurs, qui font appel aux notions d'*architectures logicielles modulaires* comme *OLE* de Microsoft et *JavaBeans* de Sun Microsystems, assurent la diffusion de documents en toute sécurité et font appel aux systèmes de gestion des droits d'auteur.

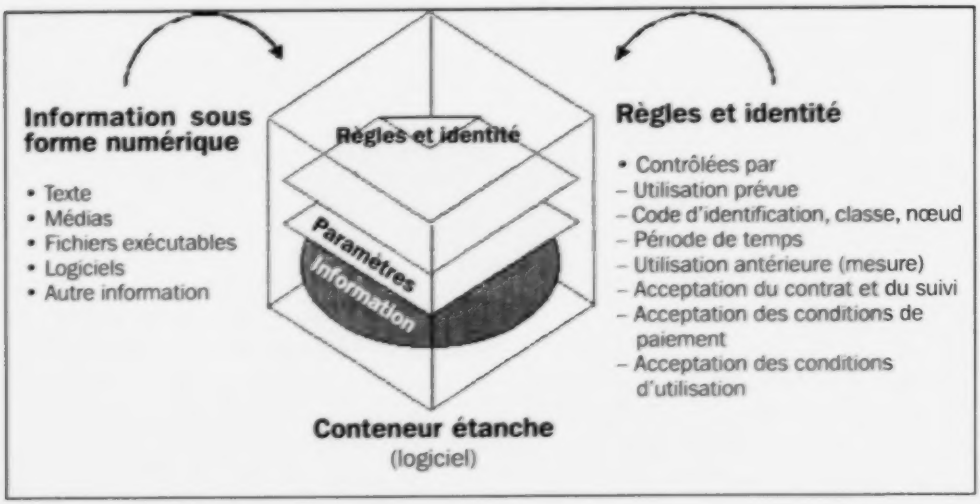
Nous présentons brièvement quelques informations publiées sur deux techniques de conteneurs, *DigiBox*[MC] d'InterTrust et *RightsPublish* de RightsMarket, pour illustrer les similitudes et la convergence générale des concepts.

4.4.1 Conteneurs *DigiBox* d'InterTrust

InterTrust offre sa technologie sous licence à ses partenaires et à des réalisateurs d'applications. Une composante centrale de sa technologie est la technique de conteneur *DigiBox*[MC], qui propose un moyen sûr d'encapsuler le contenu destiné à être géré et protégé par le système de gestion des droits d'auteur d'InterTrust. Les réalisateurs de logiciel peuvent concevoir des applications comme des serveurs, des navigateurs et des plugiciels qui mettent en œuvre le modèle *DigiBox* en incluant le code des bibliothèques de programmes fournies par InterTrust. Les éléments portant sur la gestion des droits d'auteur, par exemple le prix et les renseignements sur la licence, sont intégrés aux éléments de contenu comme les images et le texte

La protection est assurée par chiffrage tout au long du processus : le chiffrage sert à protéger le contenu des conteneurs *DigiBox*, à protéger les composantes de la gestion des droits d'auteur, que des personnes non autorisées pourraient essayer d'attaquer après avoir obtenu des données sensibles donnant accès à ces éléments, et à respecter le caractère confidentiel des renseignements sur les utilisateurs de ces données.

L'information que renferme un conteneur *DigiBox* est protégée même une fois qu'un usager y a eu accès et pendant tout le trajet du conteneur dans des réseaux non sécurisés. Les règles d'utilisation du contenu peuvent aussi être enregistrées dans le conteneur et être transmises avec l'information, ou encore voyager séparément pour un maximum de souplesse concernant ces règles après la livraison du contenu :



Conteneur étanche *Digibox*

4.4.2 *RightsPublish* de RightsMarket

RightsMarket offre une technologie de publication numérique « de bout en bout » qui peut être intégrée à un site Internet de publication existant. Le contenu numérique est chiffré et emballé dans un contenant qui interagit avec une application de RightsMarket dans l'ordinateur de l'usager et un logiciel de lecture adapté au format de fichier du contenu. (À l'heure actuelle, les formats pris en charge sont les fichiers d'images de page PDF d'*Acrobat* et les fichiers audio MP3 de *WinAmp*. En prenant en charge le format PDF, la technologie de RightsMarket reconnaît aussi toute une gamme de types d'images, de façon individuelle ou en collection.)

Un contenant *RightsPublish* (appelé *digital property* ou « bien numérique » dans le jargon de RightsMarket) possède un certain nombre de caractéristiques intéressantes :

- Le chiffrage est persistant. Le contenu est déchiffré seulement au cours d'une utilisation autorisée, et le contenu déchiffré n'est pas conservé.

- Pour obtenir un bien numérique et l'autorisation de s'en servir, l'usager accède par Internet à un serveur de RightsPublish, qui télécharge le bien numérique vers le disque de l'usager. Lorsque l'usager veut ouvrir le bien numérique en question, l'application de RightsMarket

installée dans l'ordinateur de l'usager vérifie que ce dernier a les autorisations voulues et applique les conditions d'utilisation. Par la suite, si les conditions l'autorisent, l'usager peut se servir du bien hors ligne, sans avoir besoin de rétablir chaque fois la connexion. Si le bien est acquis pour un nombre donné d'utilisations, l'ouverture hors ligne peut être limitée à un certain nombre de lectures, qui seront consignées dans le serveur de RightsPublish la prochaine fois que l'usager établira une liaison par Internet.

- Si un usager perd un bien numérique ou souhaite y accéder à partir d'un autre ordinateur, il peut en télécharger un autre exemplaire, sous réserve des conditions de licence.

- RightsMarket met en œuvre une véritable superdiffusion puisque les usagers peuvent copier ou distribuer librement les objets qu'ils ont téléchargés. Cependant, ces copies ne peuvent pas être utilisées par les personnes qui n'ont pas obtenu les autorisations voulues par le truchement du serveur de RightsPublish.

Le modèle de RightsPublish est actuellement orienté vers la prise en charge de la publication numérique « au détail », où les usagers ont une licence d'utilisation des objets numériques en tant qu'individus et paient par utilisation. Mais ce modèle pourrait être adapté à des marchés où les licences devraient avoir une portée plus étendue, par exemple pour des institutions d'enseignement comme dans le modèle *OnDisC* décrit au paragraphe 3.2.4.

5 À l'horizon

Les moyens techniques décrits dans le chapitre précédent sont conservateurs et défensifs, ce qui est compréhensible, mais l'évolution du multimédia et de sa diffusion se poursuit à un rythme très rapide, et l'on voit apparaître des applications et des modalités d'utilisation qui auraient été presque impensables il y a seulement quelques années. Dans ce dernier chapitre, nous abordons brièvement trois exemples assez différents de nouvelles techniques qui auront probablement un impact substantiel sur la manière de présenter et de protéger des images numériques. Dans chaque cas, même si ces techniques ne mettent pas spécifiquement l'accent sur la propriété intellectuelle ou la gestion des droits d'auteur, il est évident que les questions de propriété intellectuelle sont explicitement prises en considération dès les premières étapes de la conception et de la réalisation. En cela, ces innovations technologiques se démarquent de celles des années précédentes, où (comme ce fut le cas pour la normalisation des cédéroms) les questions de propriété intellectuelle n'ont été considérées qu'une fois la technologie largement utilisée.

Ces exemples représentent trois acpects différents de ce que l'on peut prévoir à court terme dans le domaine du multimédia :

- la normalisation croissante des méthodes de description d'objets numériques, qui permettra de créer des catalogues et des fonctions de recherche encore plus utiles,
- la mise au point de méthodes plus élaborées et plus puissantes de compression d'images, grâces auxquelles on pourra transmettre des images plus volumineuses, plus complexes et à plus grande résolution,
- la définition de composantes standard dans la création de nouvelles formes de présentation interactive, par l'intégration et la composition de types variés de médias.

5.1 Métadonnées sur les droits d'auteur et XML

La diffusion d'images et d'objets numériques en général requiert aussi la diffusion d'information sur ces objets, afin que les usagers puissent faire des choix et comprendre la nature et le contexte de ce qu'ils voient. On appelle *métadonnées* cette *information à propos de l'information*, semblable au contenu d'un catalogue d'une bibliothèque traditionnelle. Les métadonnées sont aussi variées que les données qu'elles décrivent, mais une norme très souple et significative concernant la syntaxe des métadonnées a récemment fait son apparition — le langage XML (*eXtensible Markup Language* ou langage de balisage extensible). Tout comme son frère HTML (*HyperText Markup Language* ou langage de balisage hypertexte) et son père SGML (*Standard Generalized Markup Language* ou langage de balisage généralisé standard), il fait appel à des balises qui encadrent des segments de texte. Exemple :

```
<format>audio/mpeg
    <extent>8 MB</extent>
    <duration>C:07:01</duration>
</format>
```

Dans les autres langages de balisage, les balises sont déterminées par la norme et n'ont de signification que pour les auteurs du balisage. En XML par contre, les balises peuvent être définies librement selon les contextes ou les applications, afin de refléter des concepts qui ont du sens pour les usagers. Ce mélange de normalisation de la syntaxe et de liberté de la sémantique facilite l'automatisation de l'échange d'information entre des systèmes et des environnements informatiques différents, tout en préservant les concepts qui ont une signification pour un groupe donné. Dans la communauté muséale, le consortium CIMI a participé à l'élaboration d'un ensemble de balises qui reposent sur des normes établies de documentation muséologique et sur les travaux antérieurs de divers producteurs de contenu sur les métadonnées élémentaires, connus sous l'appellation *Dublin Core* [Degenhart Drenth, 2001].

Dans le cas des métadonnées sur les droits d'auteur, la norme *Dublin Core* définit l'élément <rights>, qui sert à coder l'information sur les droits d'auteur, mais ne fixe pas la manière de le mettre en œuvre dans une situation donnée. Il pourrait s'agir tout simplement d'indiquer qui détient les droits et qui a une licence d'accès à l'objet :

```
<rights>
    <licensor>Encyclopédie de la musique au Canada</licensor>
    <licensee>Collège Sheridan</licensee>
    <licensee>Centre canadien du film</licensee>
</rights>
```

Le contenu de l'élément <rights> peut également être beaucoup plus élaboré et comprendre une description détaillée des conditions d'utilisation.

L'exemple de la page suivante est un court extrait d'un exemple beaucoup plus complexe de description d'une œuvre et des droits d'utilisation, tiré de la définition du langage XrML (*eXtensible rights-management Markup Language* ou langage de balisage extensible de gestion des droits d'auteur) que ContentGuard a élaboré à partir de XML [ContentGuard, 2000]. Cet exemple décrit un ouvrage électronique qui contient une image à laquelle est attachée une licence d'accès et de visionnement pendant un temps limité et à l'aide d'un appareil précis.

On ne sait pas encore si le genre de métadonnées très détaillées et logiquement complexes sur les droits proposées par ContentGuard donnera lieu à une norme acceptée (il y a des concurrents, par exemple le langage *RightsXML*[MC] de TrustData). Il n'en reste pas moins que la portée et le niveau de détail de la définition de XrML témoignent d'un intérêt croissant envers une représentation uniforme et non exclusive de données complexes sur les licences et les permissions d'utilisation dans les métadonnées d'un objet. Dans la mesure où elles facilitent le processus de gestion des droits d'auteur grâce à la mise au point d'applications qui peuvent assurer la mise en œuvre et le suivi des conditions de licence, les métadonnées sur les droits d'auteur contribueront probablement à une diffusion plus étendue d'objets sous licence.

```
<XrML>
. . .
<OBJECT type="BOOK-LIT-FORMAT"> <ID type="ISBN">8374-39384-38472</ID>
<NAME>A book of James</NAME>
</OBJECT>
        <AUTHOR>James the first</AUTHOR>
<PARTS><WORK>. . . <OBJECT type="Image"><ID type="relative">1</ID>
<NAME>Image 1: Photon Celebshots Dogs</NAME>
</OBJECT></WORK></PARTS>. . .
<RIGHTSGROUP name="Main Rights">
<DESCRIPTION>Rights granted to John Doe</DESCRIPTION>
<BUNDLE><TIME><FROM>2000-01-27T15:30</FROM><UNTIL>2000-01-27T15:30</
UNTIL>
</TIME>
<ACCESS><RIGHTSLIST><VIEW><ACCESS></RIGHTSLIST>
. . .
<OBJECT type="MS Ebook Device"><ID type="INTEL SN">Intel PII 92840-AA9-39849-
00</ID>
<NAME>Johns Computer</NAME></OBJECT>
</RIGHTSGROUP> . . .
</XrML>
```

5.2 JPEG2000

Les fondements mathématiques traditionnels d'une grande partie des techniques de compression employées à l'heure actuelle, entre autres l'algorithme de compression bien connu JPEG, sont associés à des noms aussi célèbres que ceux de Newton et de Fourier. Mais on voit poindre à l'horizon un nouvel algorithme beaucoup plus puissant, surnommé *JPEG2000*, fondé en partie sur la nouvelle mathématique des *ondelettes*. Dans les algorithmes JPEG et JPEG2000, la représentation comprimée d'une image est donnée sous forme d'une combinaison complexe de fonctions mathématiques qui saisissent de manière sélective divers aspects de l'image et qui, dans le cas d'une compression *avec perte*, omettent des caractéristiques qui ne sont pas visuellement détectables. Dans l'algorithme JPEG actuel, ces fonctions sont trigonométriques et saisissent une information sur des fréquences spatiales. Dans le cas de la compression par ondelettes, les fonctions employées sont beaucoup plus complexes : au lieu de former un spectre continu de fréquences fixes, comme dans la méthode des transformées discrètes en cosinus de l'algorithme JPEG actuel, les fonctions d'ondelettes ont des formes spécifiques choisies pour représenter de manière efficace les divers degrés et types de détails présents dans l'image [Johnson, 1999]. (En 1988, Ingrid Daubechies, mathématicienne dans les *Bell Laboratories*, a découvert une série de telles fonctions qui sont devenues le fondement d'une technique pratique d'ondelettes.)

Cette nouvelle technologie exige des décodeurs beaucoup plus complexes (et donc une plus grande puissance de calcul) que les décodeurs JPEG actuels, mais elle présente des avantages

importants [Christopulos, 2000] pour la diffusion d'images numériques, notamment :

- une amélioration de la qualité de l'image et de la fidélité des couleurs dans le traitement, avec un nombre de bits plus élevé et une taille d'image plus grande,
- une plus grande souplesse dans le choix de la qualité de la compression, depuis une compression sans perte jusqu'à des taux de compression très élevés,
- *une résolution variable, qui permet de coder avec une résolution plus grande les zones de l'image qui ont beaucoup de détails (codage ROI pour* Region Of Interest *ou zone d'intérêt),*
- un chiffrage variable appliqué à des parties choisies de l'image,
- des fichiers d'image formés de plusieurs composantes ayant des nombres de bits par pixel différents et codées avec différentes transformations de compression,
- l'emploi d'algorithmes spéciaux pour comprimer les parties textuelles d'une image, afin que la compression n'introduise pas de petites imprécisions qui nuiraient à l'exactitude de la reconnaissance optique des caractères,
- une place explicite pour des métadonnées, à propos entre autres de la gestion des droits d'auteur, incorporées dans le fichier d'image.

Les caractéristiques de JPEG2000 concernant le chiffrage et les métadonnées reflètent le constat de plus en plus répandu que l'absence d'inclusion explicite de métadonnées et de protection du contenu constituait une lacune importante des premières normes de codage de médias numériques. Les éditeurs et les diffuseurs de contenu numérique peuvent maintenant compter sur le fait que les normes plus puissantes de la nouvelle génération comprendront les structures requises pour une description contextuelle et technique appropriée du contenu, ainsi que l'identification de l'objet et l'énoncé des utilisations permises.

Quel sera l'impact de JPEG2000 sur la technologie des filigranes? Cela fait l'objet d'intenses recherches. Les premiers résultats suggèrent que les images puissent être dotées dans le « domaine des ondelettes » de filigranes invisibles [Santa Cruz, 2001] plus robustes que les filigranes conventionnels. Les filigranes pourraient donc être assez facilement intégrés à la technologie JPEG2000 et par conséquent de plus en plus employés comme technique de protection.

5.3 MPEG-4

MPEG-4 est une norme conjointe de l'ISO (Organisation internationale de normalisation) et de l'IEC (Commission électrotechnique internationale) en matière de multimédia. Elle a été élaborée suivant le même processus qui a conduit aux normes de compression très répandues MPEG-1 et MPEG-2 pour les documents vidéo. Par contre, MPEG-4 donne une description beaucoup plus complète et détaillée de la structure d'un document multimédia par rapport aux normes précédentes, qui se limitaient à des suites de bits combinant les éléments vidéo et audio. L'objectif de la norme MPEG-4 est beaucoup plus ambitieux — permettre l'intégration de l'information de production, de diffusion et d'accès au contenu dans les trois grands domaines considérés comme cruciaux pour l'avenir du multimédia : la télévision numérique, les documents graphiques de synthèse tels que les animations et les modèles, et les documents multimédias interactifs, diffusés par Internet.

La norme MPEG-4 définit des méthodes de normalisation qui peuvent servir :

- à représenter des entités de contenu oral, visuel ou audiovisuel appelées « objets médias ». Ces objets médias peuvent être naturels ou synthétiques : ils peuvent être enregistrés à l'aide d'un appareil photographique ou d'un microphone, ou être produits par ordinateur.
- à décrire la composition de ces objets en vue de la création d'objets médias composés formant des scènes audiovisuelles complexes, tout en préservant l'identité et la structure de chaque objet,
- à combiner et à harmoniser les données associées aux objets médias en vue d'une transmission efficace dans un réseau numérique,
- à permettre une interaction entre l'utilisateur et la scène audiovisuelle produite à l'extrémité destinataire.

Il est à noter que la norme MPEG-4 adopte d'emblée l'approche par objets qui a joué un rôle immense dans la production efficace de logiciels complexes et sur laquelle s'appuient les concepts de composante et de contenant décrits plus haut.

La norme MPEG-4 permet de produire un contenu beaucoup plus réutilisable et avec plus de souplesse que ce que permet la séparation actuelle des médias en techniques distinctes telles que la vidéo, les graphiques et les pages Web. Elle procure en outre aux usagers davantage de possibilités d'interaction et permet d'introduire des documents multimédias dans de nouveaux types de réseaux, notamment des réseaux à bande passante très étroite comme ceux des communications mobiles et sans fil. Pour ces raisons, la norme MPEG-4 sera probablement très intéressante pour les musées qui créent des expositions virtuelles et intègrent des documents numériques de sources multiples.

Par contre, la complexité accrue des objets médias et la variété des interactions avec l'usager que MPEG-4 permet de définir amplifient considérablement les problèmes de gestion des droits associés aux objets et à leurs diverses utilisations. La norme MPEG-4 contribue à la gestion des droits d'auteur de deux manières :

(1) Elle définit une structure d'interface cohérente entre les applications conformes à la norme MPEG-4 et les systèmes exclusifs de gestion des droits d'auteur qui font appel au chiffrage et à des données incorporées telles que des filigranes. Grâce à cette interface, il est facile d'intégrer les systèmes exclusifs de contrôle à la partie normalisée du décodeur MPEG-4. Cela devrait rendre la technologie MPEG-4 plus attrayante pour les propriétaires de contenu et contribuer ainsi à une plus grande disponibilité de la richesse présente dans les médias numériques interactifs qu'elle permet d'exploiter.

(2) Chaque objet visuel ou audio possède un descripteur qui contient une zone de donnée pour l'identification persistante de la propriété intellectuelle. Le détenteur actuel des droits sur l'objet peut ainsi être identifié par un simple accès aux bases de données appropriées. Les identificateurs seront probablement ceux de systèmes internationaux tels que l'ISAVN (*International Standard Audio-Visual Number* ou numéro normalisé international de document

audiovisuel), qui joue pour les documents audiovisuels le même rôle que l'ISBN (*International Standard Book Number* ou numéro normalisé international de livre) dans le domaine de l'édition. Si un identificateur normalisé n'est pas disponible, la propriété intellectuelle peut être identifiée par des métadonnées comme celles des exemples de la section 5.1.

Mais le maintien de la persistance d'un tel identificateur, déjà malaisé dans le cas des extraits vidéo MPEG-2, est encore plus difficile dans MPEG-4 en raison de la vaste gamme d'interactions et de transformations de média définies dans cette norme. (Voir par exemple les doutes émis par Henri Maître [1998].) Le projet MIRADOR (*MPEG-4 Intellectual Property Rights by Adducing and Ordering*), dans le cadre du programme ACTS (*Advanced Communication Technologies and Services* ou techniques et services évolués de communication) de l'Union européenne, vise la mise au point d'algorithmes de filigrane appropriés capables de survivre à ces opérations, ainsi que la conception de contremesures adéquates pour faire face à une variété d'attaques spécifiques à la norme MPEG-4. [MIRADOR, 1999]

Sources

ALA, *Digital Millennium Copyright Act, Section 1201(a) Rule*, janvier 2001.
http://www.ala.org/washoff/Rulemaking.PDF

Alchemedia Technologies, *Frequently Asked Questions*.
http://www.alchemedia.com/products/faq.html

Alsford, S., « The Canadian Museum of Civilization Stakes Out a Site in Cyberspace », dans *Museum Management and Curatorship*, vol. 13, n° 4, décembre 1994, p. 420–422.
http://www.civilisations.ca/membrs/lobby.html

AMICO, *AMICO Library University Agreement*, juin 1998.
http://www.amico.org/docs.html
http://www.amico.org/docs/AMICO.Univ.Agrmt.pdf

AMICO, *Frequently Asked Questions (FAQ)*, version 1.3, s. d.
http://www.amico.org/faq.html

Anderson, R. J., et F. A. P. Petitcolas, *Information Hiding: An Annotated Bibliography*.
http://www.cl.com.ac.uk/~fapp2/steganography/bibliography.html

Arthur, Charles, « Digital Fingerprints Protect Artwork », dans *New Scientist*, vol. 144 (12 novembre 1994), p. 24.

Baldazo, Rex, « Virtual CDs on the LAN », dans *Byte*, décembre 1995, p. 153.

Barni, M., F. Bartolini, Cappellini, et A. Piva, « Copyright Protection of Digital Images by Embedded Unperceivable Marks », dans *Image and Vision Computing*, vol. 16, 1998, p. 897–906.

Besser, H., et A. Richeson, *Protection—Watermarks, Fingerprints, Signatures*, 1996.
http://www.sims.berkeley.edu/courses/is290-1/f96/watermark.html

Bibliothèque du Congrès, *American Memory*.
http://memory.loc.gov/ammem/amhome.html

Bridgeman Art Library, *What is copyright?*, mars 1999.
http://www.bridgeman.co.uk/public/copyrights/index.jhtml?r=7203

Bridgeman Art Library, *Copyright Warning*, s. d.
http://www.bridgeman.co.uk/

Busch, Joseph, *SGML for Cultural Heritage Information*, 1995.

Cheong, Fah-Chun, *Internet Agents, Spiders, Wanderers, Brokers, and Bots*, New Riders, 1996.

Christopoulos, C. A., T. Ebrahimi et A. N. Skodras, « JPEG2000: The New Still Picture Compression Standard », dans *Proceedings on ACM multimedia 2000 workshops*, 2000. p. 45–49.
http://woodworm.cs.uml.edu/~rprice/ep/christopoulos/

Clark, Richard, « An Introduction to JPEG 2000 and Watermarking », dans *Secure Images and Image Authentication Seminar, Professional Group 4E, IEE Symposium*, 10 avril 2000.
http://www.jpeg.org/JPEG2000.htm

Cleveland, Harland, « The Twilight of Hierarchy: Speculations on the Global Information Society », dans *Information Technologies and Social Transformation*, (sous la direction de Bruce R. Guile), National Academy Press, 1985, p. 55–79.

ContentGuard, *XrML:Extensible rights Markup Language*, 2000.
http://www.xrml.org

Cox, Brad, *Superdistribution: Objects as Property on the Electronic Frontier*, Addison-Wesley, 1996.
http://www.virtualschool.edu/cox/IEEE97.html

Cox, I. J., J. Killian, T. Leighton, et T. Shamoon, « Secure Spread Spectrum Watermarking for Images, Audio and Video », dans *Proc. IEEE Internatinal Conference on Image Processing (ICIP '96)*, vol. III, septembre 1996, p. 223–226.

Degenhart Drenth, B., « Building on the mda SPECTRUM-XML DTD for collections Management Data Interchange », dans *Museums and the Web 2001*, Archives and Museum Informatics: 2001.
http://www.archimuse.com/mw2001/papers/degenhart/degenhart.html

Digimarc Corp., *Frequently Asked Questions about Digimarc Signature Technology*
http://www.digimarc.com/imaging/faq.shtml

Digimarc Corp., *MarcSpider™*, 2001.
http://www.digimarc.com/imaging/prspider.htm

« Digital Image Access Project, RLG Meeting, March 31-April 1, 1995 », dans *Archives and Museum Informatics*, vol. 9, n° 2, 1995, p. 199–209.

EVA, (Archives visuelles européennes), *Report on copyright issues*, 1999.
http://www.eva-eu.org/WP41.PDF

Fahn, Paul, *Answers to Frequently Asked Questions about Today's Cryptography*, RSA Laboratories, 1993.

Gallery V Berea College Museum.
http://www.berea.edu/GalleryV/ExhibitsHome.html

Gross, R., « Librarian of Congress Unable to Preserve Fair Use in Digital Age », dans *EFFector* , vol. 13, n° 11, décembre 2000.
http://www.eff.org/effector/

Gurrian, E., « A Blurring of Boundaries », dans *Curator*, vol. 38, n° 1, 1995. p. 31-38.

Halfhill, T., et S. Salamone, « Components Everywhere, Microsoft's Network OLE and the OMG's CORBA are competing to distribute components on your network », dans *Byte*, janvier 1996.
http://www.byte.com/art/9601/sec8/art8.htm

Hallacy, Marla, *The Dissemination of Art in the Technological Age*, 2000.
http://www.ukans.edu/~cybermom/CLJ/hallacy/hallacy.html

Harris, Lesley Ellen, *Canadian Copyright Law* , 3e édition, McGraw-Hill, 2000.

Hartung, Frank, *WWW References on Multimedia Watermarking and Data Hiding Research & Technology*, août 1999.
http: //www-nt.e-technik.uni-erlangen.de/~hartung/watermarkinglinks.html

Hartung, F., et B. Girod, « Fast Public-Key Watermarking of Compressed Video », dans *Proceedings IEEE International Conference on Image Processing (ICIP 97)*, Santa Barbara, octobre 1997, p. 528-531.

Hartung, F., J.K. Su et B. Girod, « Spread Spectrum Watermarking: Malicious Attacks and Counter-Attacks », dans *Proceedings of SPIE Vol. 3657, Security and Watermarking of Multimedia Contents*, San Jose, CA, janvier 1999. p. 147-158.

Hockin, Nora, « Canada's Digital Collections: Youth Employment Opportunities and Canadian Content On-Line », dans *Museums and the Web*, 2000.
http://www.archimuse.com/mw2000/papers/hockin/hockin.html

Hoffert, P., T. Jurenka, B. Silverman, P. Spurgeon et L. White, « Managing Intellectual Property in Digital Formats », dans *Forum for Inter-Industry Requirements for Technology-Based Intellectual Property Management*, U. S. Copyright Office and Interactive Multimedia Association, Washington, D. C., mars 1996.

IBM, *Watermarks: Protecting the image*, 1996.
http://www.research.ibm.com/image_apps/watermark.html

Internet Archive, *The Internet Archive: building an 'Internet Library'*, 15 mars 2000.
http://www.archive.org/about/index.html

Johnson, R. C., « JPEG2000 wavelet compression spec approved », dans *EE Times*, 29 décembre 1999.
http://www.eet.com/story/OEG19991228S0028
Jurenka, T., et P. Roosen-Runge, « Intercom Ontario: a residential multimedia distribution system in operation », présenté à *Multimedia to the Home, Bandwidth Battles*, Saskatoon, août 1997.

Kesse, Erich, *Negotiation and Documentation of Distribution Rights for Imaged Resources*, University of Florida, 1994.
http://palimpsest.stanford.edu/bytopic/repro/kesse/negotiat.txt

King, Brad, « Fight Rages Over Digital Rights », dans *Wired Digital*, 16 janvier 2001.
http://www.wired.com/news/politics/0,1283,41183,00.html?tw=wn20010116

Koenen, R., « MPEG4-4, Multimedia for our time », dans *IEEE Spectrum*, vol. 36, n° 2, 1999, p. 26–33.

Kutter, M., et F.A.P. Petitcolas, « A fair benchmark for image watermarking systems », dans *Proceedings of Electronic Imaging '99, Security and Watermarking of Multimedia Contents*, (P. W. et E. J. Delp, rédacteurs), Society for Imaging Science and Technology et International Society for Optical Engineering, 1999, p. 226–239.

Lehmann-Haupt, John, « Chained Melodies », dans *Think Research Magazine*, n° 2, 2000.
http://www.research.ibm.com/resources/magazine/2000/number_2/solutions200.html
Lesk, M., *Humanities and Arts on the Information Highways, Working Group Reports: The Technical Challenge for the Humanities and Arts*, Coalition for Networked Information, rapport final, 1994.
http://www.cni.org/projects/humartiway/humartiway-rpt.part2.html#tc

Licensing Still Images, Timestream Inc., 1994.

Macq, B., et J.-J. Quisquater, *Digital Images Multiresolution Encryption*, IMA IP-Workshop, 1994.
http://www.cni.org/docs/ima.ip-workshop/Macq.Quisquater.html

Maître, H., *Image Waternarking, Why is watermarking a hard problem*, Atelier Corée–France sur le multimédia, Séoul, 6–9 juillet 1998.

Microsoft, *Window media Rights Manager 7*, mai 2000.
http://www.microsoft.com/windows/windowmedia/enWM7/rightsmanager.asp

Mintzer,F., G. Braudaway, F. Girodano, J. Lee et K. Magerlein, *Populating the Hermitage Museum's New Web Site*, Rapport de recherche IBM, RC21753 (97990), IBM, 2000.

MIRADOR, *MPEG-4 Intellectual Property Rights by Adducing and Ordering*, ACTS, 1999.
http://www.infowin.org/ACTS/RUS/PROJECTS/ac302.htm

Musée de l'Hermitage, Saint-Pétersbourg, Russie. *Digital Hermitage Project*.
http://www.hermitagemuseum.org/

National Palace Museum — Taiwan, *Virtual Tours*.
http://www.npm.gov.tw/english/live/live.htm

Norman, S., « Copyright in the Global Information Infrastructure (GII), Mexico, 22-24 May 1995 », dans *IFLA Journal*, vol. 21, n° 3, 1995.

OMPI (Organisation mondiale de la propriété intellectuelle), Traité de l'OMPI sur le droit d'auteur, 1996.
http://www.wipo.org/fre/diplconf/distrib/94dc.htm

Orlowski, A., « The Open PC is dead - start praying, says HD guru », dans *The Register*, n° 7, mars 2001.
http://www.theregister.co.uk/content/2/17419.html

Parcs Canada, *Utilisation des illustrations*
http://www.parkscanada.gc.ca/avis-notice_f.asp

Petitcolas, F., *Weakness of Existing Watermarking Schemes, StirMark*, 1997.
http://www.cl.cam.ac.uk/~fapp2/watermarking/image_watermarking/stirmark/index.html

Petitcolas, F., *Watermarking and Steganography — Companies & Products*, Université de Cambridge, 1998.
http://www.cl.cam.ac.uk/~fapp2/watermarking/products.html

Petitcolas, F., *The information hiding homepage - digital watermarking & steganography*, 2000.
http://www.cl.cam.ac.uk/~fapp2/steganography/

Petitcolas, F., et R. Anderson, « Evaluation of copyright marking systems », dans *Proceedings of IEEE Multimedia Systems*, vol. 1, 1999, p. 574–579.

Réseau canadien d'information sur le patrimoine, *Licenses de CD-ROM pour les musées — Accords types. Édition canadienne conforme au code civil du Québec, Édition conforme à la common law, Canada*, Travaux publics et Services gouvernementaux Canada, 1997.

Réseau canadien d'information sur le patrimoine, « *Numérisez vos collections* — Cours sur la numérisation — Sommaire », 2001.
http://www.rcip.gc.ca/Francais/Contenu_Numerique/Numerisez_Collections/index.html

Resnick, P. « Platform for Internet Content Selection », dans *W3C*, janvier 1998.
http://www.w3.org/PICS/

Reuters, *Gates' Corbis buys giant photo agency*, 15 juin 1999.
http://www.zdnet.com/zdnn/stories/0,4586,2276787,00.html

RightsMarket™, document technique.
Rottenberg, B., et R. Pantalony, « Moral Rights and Exhibition Rights, A Canadian Museum's Perspective » dans *Copyright and Fair Use, The Great Image Debate, Visual Resources*, Gorden and Breach, 1997, p. 409.

Rowan, G., « Secure computer files may not be so safe », dans le *Globe & Mail*, 4 décembre 1997, p. B8.

Santa Cruz, Diego, *Watermark tests in JPEG2000*, Laboratoire de traitement du signal, Institut fédéral suisse de Technologie, 1999.
http://eurostill.epfl.ch/~ebrahimi/JPEG2000Seminar/SantaCruz.pdf

Schneier, B., *Secrets and Lies, Digital Security in a Networked World*, Wiley, 2000.

Schneier B., « Hard-Drive-Embedded Copy Protection », dans *Crypto-Gram*, 15 février 2001.
http://www.counterpane.com/crypto-gram-0102.html#1

Schofield, J., « The Fight for Knowledge », dans *Macleans*, 4 décembre 2000.
http://www.macleans.html.ca/xta-asp/storynav.asp?/2000/12/04/Education/44105.shtml

Smith, B., et D. Semperger, « The Power of Digital Archiving with Photo CD », dans *Spectra*, vol. 22. n° 3, hiver 1994–1995, p. 15.

Snow, M., « License to Kill? Copyright Ownership and Fair Use in Age of Licensing », dans *VRA*, juillet 1997.
http://www.oberlin.edu/~art/vra/license.html

Spurgeon, G. (<gspurgeo@SPIFF.CHIN.GC.CA>), « Re: artists' rights in Canada », message dans *MUSEUM-L*, 11 avril 1996.

Stefik, M., « Trusted Systems », dans *Scientific American*, mars 1997.
http://www.sciam.com/0397issue/0397stefik.html

Stewart, Doug. « Masterieces on View », dans *IBM Research Magazine*, n° 2, 1999
http://www.research.ibm.com/resources/magazine/1999/number_2/solutions299.html
Storm, W., « The value of integrated access to print and AV collections », dans *IFLA Journal*, vol 21, n° 3, 1995. p. 203–210.

Strong, William S., « Copyright in the New World of Electronic Publishing », dans *Electronic Publishing Issues II, Association of American University Presses, (AAUP) Annual Meeting*, Washington, D.C., 17 juin 1994.
http://www.press.umich.edu/jep/works/strong.copyright.html

Szczesny, Barry G., *What's Happening in Washington*, exposé présenté à la réunion annuelle de l'*American Association of Museums*, avril 1999.
http://www.panix.com/~squigle/rarin/corel2.html

Tomlin, Judith, *La Numérisation au Musée canadien des civilisations*, exposé présenté à la réunion annuelle du Comité international pour la documentation (CIDOC) du Conseil international des musées, Ottawa, ON 23 et 24 août 2000.
http://w..v.chin.gc.ca/Resources/Cidoc/French/index.html

Trant, J., « The Museum Educational Site Licensing Project », dans *Spectra*, vol. 22, hiver 1994–1995, p. 19–21.
http://ei.cs.vt.edu/~mm/cache/Trant.htm

Université de l'Alberta, licence de site d'AMICO
http://ej.library.ualberta.ca/database/index.cfm?ID=71

Van Eyck Project, VASARI (*Visual Arts Network for the Exchange of Cultural Knowledge*)
http://www.vasari.co.uk/van_eyck.htm

van Horik, René, « Archives and Photographs: the 'European Visual Archive' Project (EVA) », dans *Cultivate Interactive*, n° 3, 2001.
http://www.cultivate-int.org/issue3/eva/

Voyatzis, G., et I. Pitas, « Protecting Digital-Image Copyrights: A Framework », dans *IEEE Computer Graphics and Applications*, janvier–février 1999, p. 18–24.

Walter, Mark, « Keeping tabs on the taking and selling of digital images », dans *Seybold Report on Publishing Systems*, vol. 24, 2 janvier 1995, p. 21 et suivantes.

Weber, Hartmut, « Opto-Electronic Storage—An Alternative to Filming? », dans le bulletin de la *Commission on Preservation and Access*, février 1993.

Zhao, J., « Applying Digital Watermarking Techniques to Online Multimedia Commerce », dans *Proc. of the International Conference on Imaging Science, Systems, and Applications (CISSA '97)*, 1997.
http://syscop.igd.fhg.de/Publications/Zhao97a.pdf

Fournisseurs et organismes

Alchemedia Technologies, Inc.
300 De Haro Street, Suite 334, San Francisco, CA 94103, États-Unis
Téléphone : 1-800-561-8295
http://www.alchemedia.com/

Bridgeman Art Library
17-19 Garway Road, London W2 4PH, Royaume-Uni
Téléphone : +44 (0)20 7727 4065
Courriel : info@bridgeman.co.uk
http://www.bridgeman.co.uk/

Cognicity
7171 Ohms Lane, Suite 100
24947 Lorena Drive Minneapolis, MN 55439, États-Unis
Téléphone : 952-841-7100
Télécopie : 952-841-7101
Courriel : info@cognicity.com
http://www.cognicity.com/

ContentGuard, Inc.
6500 Rock Spring Drive, Suite 110 Bethesda, MD 20817-1105, États-Unis
Téléphone : 1-800-870-0705 (aux États-Unis)
Téléphone : 1-650-813-7886 (de l'extérieur des États-Unis)
http://www.contentguard.com

Corbis Corporation
15395 SE 30th Place, #300, Bellevue, WA 98007, États-Unis
Téléphone : (206) 641-4505
Télécopie : (206) 643-9740
http://www.corbis.com

Dryden Aircraft Research Aircraft Photo Archive
Courriel : robert.binkley@dfrc.nasa.gov
http://www.dfrc.nasa.gov/gallery/photo/

Fraunhofer-Institut für Graphische Datenverarbeitung
Rundeturmstraße 6, D- 64283 Darmstadt, Al;emagne
Téléphone : ++49 / 6151 / 155-0
Télécopie :++49 / 6151 / 155-199
http://www.igd.fhg.de/
Dr. Eckard Koch
Téléphone : (06151) 155-147
Télécopie : (06151) 155-199
Courriel : ekoch@igd.fhg.de

Groupe de recherche OnDisC
Sheridan College, Office of Research Development, 407 Iroquois Shore Road, Rm. A-23 Oakville (Ontario), Canada
http:// www.ondisc.ca

IBM DB2 Digital Library Project
http://www-4.ibm.com/software/is/dig-lib/casestudy.html

InterTrust Technologies Corporation
4750 Patrick Henry Drive Santa Clara, CA 95054, États-Unis
Téléphone : 1 (800) 393-2272 (aux États-Unis)
Téléphone : + 1 (408) 855-0100 (de l'extérieur des États-Unis)
Télécopie : + 1 (408) 855-0144
Courriel : info@intertrust.com
http://www.intertrust.com

MediaSec Technologies LLC
321 South Main Street, Suite 100, Providence, RI 02903, États-Unis
Téléphone : +1-401-831-2479
Télécopie : +1-401-453-0444
Courriel : info@mediasec.com
http://www.mediasec.com

Projet BELLE
http://www.netera.ca/belle

RightsMarket
500, 700 - 4th Avenue S. W., Calgary (Alberta) T2P 3J4, Canada
Téléphone : (403) 571-1835
Télécopie : (403) 571-1838
Ventes : 1 (877) 543-3556
Courriel : sales@rightsmarket.com
http://www.rightsmarket.com/

Superdistribution[MC], Inc.
11800 Sunrise Valley drive, Suite 1000, Reston, Virginia, 20191, États-Unis
Téléphone : 703-244-0986
Courriel : info@superdistributed.com
Chef de l'exploitation : Finley Foster
Courriel : ffoster@superdistributed.com
http://superdistributed.com

VASARI Enterprises
44A Florence Road, Fleet, Hampshire, GU13 9LQ, Royaume-Uni
Téléphone : + 44 [0] 20 8977 7858
Télécopie : + 44 [0] 20 8943 9256
Courriel : jamesrhemsley@cix.co.uk
http://www.vasari.co.uk

Vyou.com
2 North Second Street, Suite 1450, San Jose, California 95113, États-Unis
Téléphone : (408) 287-4200
Télécopie : (408) 279-5643
Courriel : info@vyou.com
http://www.vyou.com